Ovum
TMT intelligence | informa

Making Sense of Compliance: MIFID II and Financial Trading

Best practices for compliance and corporate governance

Publication Date: June 18, 2018

Rik Turner

Ovum view

Summary

MiFID II is a piece of European Union (EU) regulation that came into force in January 2018 with compliance requirements for the financial sector across the organization's 28 member states and beyond. In this white paper, Ovum looks at the impact of the regulation on firms in the capital markets, and how technology can help them comply.

What is MiFID II?

The EU adopted its Markets in Financial Instruments Directive (MiFID) in 2004, with legislation coming into force across member states in November 2007. MiFID established a regulatory framework for the provision of investment services in financial instruments, such as brokerage, advice, dealing, portfolio management, and underwriting, for the operation of regulated markets. It also defined the powers and duties of national competent authorities in relation to these activities.

In October 2011, the European Commission adopted a legislative proposal for the revision of MiFID, designed to take into account developments in the trading environment since 2007, and in light of the financial crisis of 2008/9, to improve the functioning of financial markets, making them more efficient, resilient, and transparent.

The proposed structure of this revision took the form of a revised directive ("MiFID II") as well as a new Regulation ("MiFIR"), with the difference that a directive requires transposition into law by the parliaments of each of the member states, whereas a regulation comes into force across the entire EU as soon as it is passed by the competent EU authorities, the European Council and Parliament.

MiFID II and MiFIR were adopted by the European Parliament on April 15, 2014, and by the Council of the European Union on May 13, 2014, proceeding to publication in the EU Official Journal on June 12, 2014. There were delays in their actual implementation, in particular in March 2016, when the parliament asked the EU's capital markets regulator, the European Securities and Markets Authority (ESMA), to rewrite three technical standards governing trading in commodities, exemptions for companies providing ancillary market services, and displaying prices in fixed income markets.

The question of MiFID II's extraterritoriality (the degree to which it applies to non-EU firms) is a knotty one in that it has multiple dimensions. Companies headquartered outside the EU but trading within the region will be covered, for instance, by the regulation's dealing commission rules, and if they are executing orders for EU-based clients, or executing in dual-listed financial instruments.

Furthermore, there are some obligations on the non-EU entity that will apply directly, in areas such as research and best execution, while others will be indirect. EU-based counterparties will make them a requirement of transacting business in order that they, the counterparties, remain compliant.

This is the case in transaction reporting, trade reconstruction, and trade surveillance, all of which require the non-EU entities to provide electronic trade reports in a format compatible with the EU counterparties' transaction reporting systems, as well as audit trails so that they can meet their market abuse/trade surveillance obligations.

What is MiFID II's impact on market participants?

MiFID II represents a sea change in the world of non-equities, particularly those that have never before been traded on exchanges. Many of these instruments are now exchange-traded and subject to similar regulatory oversight to equities.

The revision of MiFID also expands the regulation of equities whereby voice recording requirements are extended to mobile calls. It also requires data to be recorded and stored on all communications (voice and non-voice) pertaining to an actual and potential trade, expanding the scope beyond the actual traders to all participants associated with a transaction, such as independent financial advisers (IFAs).

In its drive for greater transparency, MiFID II introduces:

- thresholds for the pre-trade and post-trade transparency regimes extended to equity-like instruments, bonds, derivatives, structured finance products, and emission allowances
- a liquidity assessment for non-equity instruments
- a trading obligation for shares and certain derivatives to be traded only on regulated platforms, and in the case of shares, systematic internalizers instead of over-the-counter
- a double volume cap mechanism to limit dark trading and reshape the use of waivers for shares and equity-like instruments
- new reporting requirements for commodity derivatives.

The directive further makes provision for stronger protection for investors in the capital markets by requiring a higher standard of disclosure to demonstrate best execution.

All of these new requirements, together with the fact that they are being applied to an expanded range of asset classes, means a huge increase in the volume and types of data to be recorded and stored in order to comply with MiFID II. This situation presents a significant challenge to both market participants and regulators, whose job it is to sift through the mountains of data to determine whether companies have complied or not.

Market participants also face MAR and MAD II since July 2016

In addition to the recast MiFID that came into force at the beginning of 2018, the EU has also beefed up its market abuse regime with two pieces of legislation, namely the Market Abuse Regulation (MAR) and the revamped Market Abuse Directive (MAD II), the latter of which updates its eponymous predecessor from 2003. Both came into force from July 2016.

The impact of the regulation is that:

- Existing market abuse rules are broadened to include abuse on the electronic trading platforms that have proliferated in recent years.
- Abusive strategies enacted through high-frequency trading are the subject of explicit prohibition.
- Manipulation of benchmarks such as LIBOR is considered market abuse and culprits are subject to heavy fines.
- Market abuse taking place across both commodity and related derivative markets is prohibited, while cooperation between financial and commodity regulators is reinforced.

- The deterrent effect of the legislation is far greater than that of its predecessor (MAD I), with potential fines of up to three times the profit made from market abuse, or at least 15% of turnover. Individual member states can decide to go beyond this minimum.

Meanwhile, the directive's adoption means that:

- There are now common EU definitions of market abuse offences such as insider dealing, unlawful disclosure of information, and market manipulation.
- There is also a common set of criminal sanctions, including fines and imprisonment of four years for insider dealing/market manipulation and two years for unlawful disclosure of inside information.
- Legal persons (both individuals and companies) will be held liable for market abuses.
- Member states must establish jurisdiction for these offences if they occur in their country or the offender is a national.
- Member states need to ensure that judicial and law enforcement authorities dealing with these highly complex cases receive the appropriate training.

These regulatory moves are mentioned here because in broadening the scope of the market abuse regime to more asset classes and more trading venues, they create an increased requirement for record keeping, including voice communications, dovetailing with what MiFID II and MiFIR introduced.

Best practices for compliance and corporate governance

Data should be held in a searchable and identifiable format. In the case of voice calls, companies should strive for clear, listenable audio files in which words and phrases can be made out. There will, of course, be a need to determine which of the parties on the call said what, which is not immediately obvious on a mono recording. The argument that "it was a poor line" will risk incurring the wrath of the regulators.

Stereo separation

For this reason, stereo separation of the people speaking on a call is required. While physical stereo separation is an attribute of recording systems themselves, there is also a need for software-based separation of the speakers in so-called monaural recordings, where the physical separation has not been carried out at the time of recording.

Furthermore, given their impact on the quality of voice transcription and playback, both audio compression and the mixing of voice channels that typically happens on trading turrets should be turned off.

The timeliness of compliance actions

The primary driver for investment in the systems to capture and retain all the necessary data will of course be compliance with the regulation itself, so that as and when a regulator comes knocking, an enterprise will be ready with all the appropriate information to support an investigation. And by committing resources to comply, companies avoid the kinds of financial and reputational penalties inherent in noncompliance. There is also a growing requirement to comply in a timely fashion, because regulators can impose ever tighter deadlines for presenting the data pertaining to their investigations, with financial and reputational penalties for failing to meet them.

Staying one step ahead of the regulator

However, there is also a strong case for getting ahead of the authorities. Having made the investment in time and money to install a compliant infrastructure, companies should consider applying their own in-house analytical capabilities to the data, with a view to detecting any deviation from acceptable business practices before it escalates into the subject of a regulatory action.

This could be carried out on data either locally or in the cloud, but either way, companies should have the ability to gather and analyze data from multiple physical repositories, both cloud and on-premises, and provide holistic analytics from a single application.

Speech, text, and desktop analytics

Speech analytics is a vital part of the armory for both regulators and the companies seeking to comply with the regulations. It can be used to track key words and phrases in conversations, helping anyone investigating activities on the trading floor to home in on specific recordings and thereafter to track the activities of particular traders.

Beyond that, companies should consider investing in both text and desktop analytics. The former enables them to look at the contents of SMS messages to and from the mobile phones of their recorded employees, while the latter extends the analytical capability to employees' use of systems, applications, and processes on their computers. The combination of all three analytical approaches is required to get a full picture of communications and actions related to trading and pre-trading activities.

Identity analytics

Identity analytics, the use of voice biometrics technology to accurately identify the speakers in calls, has a role to play here. On calls that have been recorded and are used in investigations, whether by the regulators or by the companies themselves, it will speed the process of identifying the company's employees, such as the trader, by comparing the voices on the call with pre-recorded "voiceprints." Equally, all companies in the markets maintain blacklists of individuals with whom it is forbidden to trade, and if voiceprints of these people can also be obtained, voice biometrics will be able to determine that any business with them must be blocked, reducing both financial and regulatory risks.

It is worth mentioning in this context that voice biometrics works across all devices, mobile phones as well as turret and simple desk phones. This is important because MiFID II expands compliance requirements to the mobile domain.

How can technology help with MiFID II compliance?

To comply with MiFID II, companies need to record and store all the data relating to a transaction in both equities and a wide range of non-equities such as bonds, derivatives, and carbon emissions. This includes all non-voice data such as emails, IM, and SMS messages, plus all voice calls, fixed and mobile, with audio recordings needing to be kept for five years. The regulation covers not only the actual traders who executed a trade and their counterparty, but also all the other people associated with that transaction, which will include any advisers who counseled the customer, market analysts, and so on.

The sponsor of this report, Verint Systems, develops technology that can help navigate complex regulations such as MiFID II. Verint has undertaken a deep analysis of the new requirements and has set out to “re-invent” compliance based on six core themes:

Communications are Omnichannel and Unified

Communication is no longer just voice - it’s chat, screen share, file transfers and video. The optionality around communications channels continues to grow, and with it the complexity of recording. Verint offers automated, secure compliance capture functionality across a range of leading real-time communications and collaboration environments.

Verint offers an integrated, secure compliance recording solution to capture voice, SMS, instant messaging, screen and application share, video conferencing, file transfer and other means of collaboration that come into play in financial trading and back-office environments. The platform’s versatility is reflected through its strong cross-platform compatibility - recording a range of modalities across multiple channels including market-leading unified communications and collaboration, trading turret, PBX, and public mobile networks.

At the same time, Verint Speech Analytics can search, process, analyze, and report on 100 percent of recorded calls, to help expedite investigations while eliminating the need for costly, time-consuming manual sampling and transcriptions. Your compliance officers and analysts can gain faster, deeper insight into trading room conversations and quickly find the ones that can put your organization at risk.

Protecting proprietary investments through open APIs

Verint’s strategy is about simplification, based on open APIs to seamlessly integrate with your existing infrastructure. The framework provides open, elemental capability that allows clients the freedom of choice, whilst ensuring the data that is captured belongs to them, and is readily available in a usable format as a proof of evidence upon the regulator’s request.

Be Proactive, not Reactive

Verint recognises that while capturing (active compliance), archiving and analysing data (reactive compliance) accurately is critical, prevention is better than applying corrective measures once a failure occurs. Verint offers a change-oriented, forward-looking approach and is focused on delivering unique proactive compliance capabilities that help avoid potential breaches.

A core part of the Verint platform is the **Ethical Wall** that is proactively (through predefined policy) able to block fraudulent calls from happening and can set controls around file attachments and user presence. Companies are now encouraged to take proactive measures to help prevent the negative consequences of noncompliance. By operating a robust, proactive **Policy Engine**, multiple dashboards and with alerting options, Verint can allow a company to be fully in control and aware of a system’s health, status and performance at any given time, while constantly verifying its adherence to policies.

Fostering Sustainability and Transformation

Applying best-of-breed technology is only one part of the compliance challenge. The ability for businesses to evolve and transform without risk and deliver sustainable support and focused services is equally important. Financial firms must be able to take control over change of regulated users and licenses, otherwise the solution deployed might run the risk of losing its adherence to the regulations in place.

Following installation, companies require the assurance that their underlying communications and recording infrastructure is fully operational and continues to meet compliance requirements while mitigating the risk of costly disruptions. The Verint Automated Verification performs system tests across multiple vendor platforms, applications and communication paths. This vendor-independent solution actively checks for issues and proactively simulates user transactions to validate the operation, configuration, and performance of applications, communication flows, and interaction recording.

Putting Automation to Work for You

Businesses can only navigate the regulatory complexity and mitigate risk by implementing automation that is able to regularly verify compliance, enforce policies, monitor communications and validate the communications and recording infrastructure. Removing human error, replacing time-consuming and repetitive tasks, and improving the efficiency of IT and Compliance teams are cornerstones of a successful compliance program.

One of the key challenges companies face when looking to manage complex compliance requests is streamlining time-consuming activities, such as sampling conversations. Using automated, auditable capture and processing interaction data removes the need to handle these tasks manually, leading to increased efficiency and cost reductions. Verint manages all aspects of collaboration compliance in one place, while offering the functionality to address requirements including search and replay, categorization, access control, legal hold, and data retention.

Powering a Compliance Alliance

By partnering with leading players from the RegTech and FinTech space, Verint can give companies access to a holistic compliance solutions ecosystem that brings the best of all worlds without locking them down into a single proprietary vendor.

Appendix

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

CONTACT US

www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo