MiFID II: Setting a Mobile Policy for Compliance and Trading Business
INTRODUCTION

The EU’s impending MiFID II regulation includes provisions governing the recording of trading-related electronic and voice communications. The new rules – which come into effect January 3, 2018 – go further than earlier regulations, introducing highly prescriptive rules about recording, storing and accessing all voice and electronic communications that may pertain to a transaction, a broader brush than earlier requirements to record and store communications that resulted in a trade.

Financial institutions have long been aware of the compliance issues around e-comms and trading room voice recording – particularly as they apply to financial crime. But fewer understand how the new MiFID II requirements will impact their employees’ use of mobile devices, according to a survey of a dozen communications and compliance executives at financial institutions conducted by A-Team Group’s Intelligent Trading Technology.

Financial institutions need to assess how the new provisions will affect them and their trading and investment staff, and determine what mobile communications policy they implement. While some firms are looking to take a ‘manage by policy’ approach – in essence, implementing blanket restrictions on mobile device use deemed ‘risky’ – the complexity of the current mobile landscape makes this approach ineffectual at best and potentially damaging at worst.

Global Implications

As with other aspects of MiFID II, the regulation’s mobile recording provisions apply across all asset classes – expanding the remit of its predecessor, MiFID I – and in all 28 EU jurisdictions. Nor are they restricted in their application to EU member firms: MiFID II has implications for any entity in the world doing business with counterparties based or operating in the EU.

Compliance with MiFID II’s record keeping requirements is challenging, with financial institutions obliged to record, store, retrieve large quantities of immutable recordings for five, and in some cases seven, years after the original recording. Applying the requirements to mobile communications adds complexity, particularly as firms strive to implement cost-saving ‘bring your own device’ policies, which by definition make compliance and security more difficult.
This all presents a practical / technological challenge, but it also requires a robust mobile policy and education of affected personnel. Compliance will also require strong governance to ensure affected staff know and play by the rules.

This challenge is complicated by the recent growth in the number of communications channels used by traders, portfolio managers and analysts to communicate with clients and others involved in the trading and investment process. As well as voice, mobile phones are used for a multitude of electronic channels, including SMS messaging, Skype and WhatsApp, to name but a few.

According to the Intelligent Trading Technology survey, the industry isn’t fully sure of its obligations under MiFID II. In a recent poll, 50% of respondents said they were aware of the new requirements, with the same proportion reporting that they expected to comply satisfactorily and on time.

Yet survey respondents identified several areas of concern, with 45% suggesting records retrieval presented the greatest challenge and 40% implementing voice surveillance technology. Other key challenges included setting policy and archiving records.

But there are many more factors to consider when designing and implementing a mobile surveillance system and a policy that governs it. This paper will explain the regulatory requirement for mobile communications under MiFID II, and identify key issues for achieving compliance. It outlines considerations for implementing a technological solution, and discusses how best to put in place a robust mobile policy and governance programme.
THE REGULATORY IMPERATIVE

The requirement to monitor and retain details of trading-related voice and electronic communications under MiFID II raises the bar in scope, magnitude and jurisdictional range. It also looks to enforce the kind of communications monitoring envisaged by the US Dodd-Frank Act, which has experienced significant pushback from the industry since its introduction in 2014.

For its part, ESMA says the monitoring of trading-related communications will aid in ensuring firms are adhering to their regulatory obligations under MiFID II.

Specifically, “it will assist the firm in meeting its wider regulatory obligations, which include but are not limited to having policies and procedures in place in respect of its client order handling, best execution, own account dealing obligations and the deterrence and detection of market abuse.”

To that end, regulators will require firms to have the ability to reconstruct trading conversations that are faithful to their original chronology across all appropriate communications media and channels, including mobile.

MiFID II goes further than its predecessor MiFID I and the existing EU Market Abuse Regulation (MAR) by requiring capture / recording of all communications that could relate to a transaction (as prescribed by Article 16[7] of MiFID II), whether or not the transaction takes place. (Earlier regulations, like MiFID I, the UK Financial Conduct Authority’s COB 11.7 and MAR required capture of communications only related to a completed transaction.)

Communication ‘Relating to’ Orders

ESMA’s latest clarification on this issue – in a Q&A published in July 2017, – states: “Internal telephone conversations and electronic communications that ‘are intended to result in transactions’ or ‘relate to’ the reception and transmission of orders, execution of orders on behalf of clients and dealing on own account are subject to the MiFID II Article 16(7) recording requirement. Recital 57 of MiFID II sets out that: ‘such records should ensure that there is evidence to prove the terms of any orders given by clients and its correspondence with transactions executed by the investment firms, as well as to detect any behaviour that may have relevance in terms of market abuse, including when firms deal on own account.’”
Article 16(7) requires the recording and storage of “telephone conversations or electronic communications relating to transactions concluded when dealing on own account and the provision of client order services that relate to the reception, transmission and execution of orders … even if those conversations or communications do not result in the conclusion of such transactions”. In practical terms, this translates to a need to record and archive all communications about potential transactions even if not completed, and possibly, therefore even future transactions.

According to ESMA, “Internal telephone conversations and electronic communications that ‘are intended to result in transactions’ or ‘relate to’ the reception and transmission of orders, execution of orders on behalf of clients and dealing on own account are subject to the MiFID II Article 16(7) recording requirement.”

Sales and Research Calls

ESMA offers the following example: “Such records should include conversations or communications by which the sales desk will require a quote from the trading desk on a financial instrument before concluding a transaction with a client. It may also include conversations or communications that are within scope and made to or from the sales and research desks,” (our italics).

Clearly, this requirement applies to the traditional fixed lines used by traders and analysts in and around the trading room environment. But it also applies to mobile where devices are used for trading-relating communication. While some firms – particularly those attempting to apply a ‘manage by policy’ stance on mobile use – hope to circumvent mobile use for trading and investment business, practitioners concede that it’s impossible to completely preclude this usage, with the potential for putting the firm at risk.

As such, for staff whose activities fall within the scope of the directive, firms need to ensure compliance with several key MiFID II provisions. All trading-related communications carried out from a mobile device needs to be recorded. This includes voice, SMS (text messaging) and any phone- or tablet-based instant or other messaging application used in trading-related conversations, such as chat, email, Bloomberg Mail/Messaging, Skype and others.

Also key to compliance is storage of records, and archiving appropriately to ensure ease of access in response to a regulatory enquiry. ESMA says “Firms are required to keep records produced
under Article 16(7) of MiFID II for five years, with the extension to seven years, if requested by the competent authority.” Extensions can occur, it says, where a competent authority undertakes “complicated regulatory investigations in the course of exercising its supervisory powers” or where an authority is conducting an investigation on an issue dating several years prior to the start of the inquiry.”

Archive retrieval must be fast, precise and complete, which requires indexing and linking of relevant records. All records must be immutable/durable, meaning that records must remain intact once they are recorded. MiFID II specifies a time-stamp granularity for voice-based trading of one second, with maximum divergence from the benchmark Coordinated Universal Time (UTC) of one second. Firms need to ensure this level of granularity across all voice channels used in trading and client conversations.

**Recording All Conversations**

In short, MiFID II effectively requires firms to record all conversations – internal and external – pertaining to any aspect of trading, whether for the firm’s own account or on a client account, as well as all related communications, from supplying research and advice to providing a quote.

Finally, MiFID II also goes further than its predecessors by requiring that surveillance be proactive. It is no longer sufficient for firms merely to respond to regulatory enquiries. Rather, they need a mobile policy in place, must demonstrate to regulators that its employees understand it, and are required proactively to record and capture all communications relating to trading business.

As already mentioned, the marketplace itself appears split in its readiness for the MiFID II mobile surveillance challenge, with 50% of respondents to a recent Intelligent Trading Technology poll saying they understand the requirements for surveillance and a further 50% indicating they were prepared to implement systems to meet those requirements.

But drilling down into the requirements as they pertain to mobile voice and messaging reveals a number of specific challenges that need to be addressed in order to attain compliance with MiFID II’s trading communications surveillance obligations.
Technology Challenges

As discussed above, the requirements introduced by MiFID II extend those already in place and governed by other regulations including MiFID I, MAR as well as CFTC (Dodd-Frank) and the FCA’s 2011 COB 11.7. As such, many financial institutions have a base surveillance capability in place, often revolving around the voice recording functionality deployed in trading rooms.

The technical resources required to meet the new obligations may, in fact, be relatively straightforward, with a few exceptions discussed below. But implementation may be complicated, particularly when a solution needs to cover multiple communication systems, including trader turrets, mobile handsets or network-level devices, with different formats and time sequences.

For those seeking to extend an existing platform to accommodate mobile communications, there will be issues around re-engineering to create an architecture that can cover all requirements. For those seeking a new platform, there is the risk of disruption and additional expense.

Recording Across Systems

Size and function of organisation may also factor into technological approach taken. Tier 1 and larger Tier 2 institutions tend to prefer onsite solutions, which typically means extending their existing recording storage infrastructure to enable recording of mobile communications and fixed line voice. Smaller institutions, meanwhile, don’t have the internal resource to tend to more complex internal infrastructures, making cloud-based solutions more attractive to them.

Whichever path is taken, the technological solution needs to be able to record messages across systems, store it in a secure and durable way, and allow flexible access to meet retrievability requirements. On top of that, surveillance may require capabilities such as voice-to-text transcription, keyword detection and pattern recognition, each bringing its own challenges.

At the very least, the system needs to be capable of recording voice, and other communications media like SMS and IM, used via mobile devices. Respondents to the Intelligent Trading Technology survey reported some specific technical hurdles to achieving this.
For instance, some had issues with handling SMS. “We are struggling to find a provider that can lock down and keep SMS messages securely, and make the data able to be searched, retrieved and archived,” said the compliance director at the London offices of a Tier 1 US sell-side institution. “Finding a vendor working across the UK and our 27 other jurisdictions is impossible, so we will have to use multiple vendors.”

This issue is exacerbated by the fact that while perhaps 80% of regulated users at most banking institutions are clustered around key centres in the UK, Germany, France, Spain and elsewhere, many firms also have so-called ‘long tails’ of handfuls of users based in Liechtenstein, Gibraltar and other specialist European enclaves. Needless to say, these users need to be covered by any policy – and any solution – adopted by the firm, which can be expensive for such small numbers.

**BYOD Issues**

Another, a senior compliance manager at a Tier 1 European investment management firm, said he was able to capture and store all SMS messaging from corporate mobile devices, but was unable to do so for employees’ own BYOD phones. Use of these were banned under the firm’s mobile management policy, he said, so the issue was one of enforcing the policy.

Security was another major issue raised by survey respondents, with two-thirds of respondents citing it as one of their top two priorities with respect to mobile policy. The decline in usage of the BlackBerry Handset – widely held to be the most secure device on the market – was flagged as a security issue by survey respondents. Moreover, some firms said they are restricting use of the popular Android and iPhone platforms – deemed less secure than BlackBerry – using Mobile Device Management (MDM) platforms, to avoid compliance headaches.

For some of those surveyed, security considerations around BYOD have led them to reconsider recent shifts toward allowing employees use their own devices. Said one: “There’s been an industry drive toward bring your own device as it saves money for the bank. But due to security concerns, some firms have gone back to supplying devices for the business – we’re still considering that – so they’ve gone full circle.”
Another Tier 1 firm reported foregoing security in favour of savings. “Our very successful pursuit of cost reduction through the implementation of a BYOD strategy has left us potential exposed in some parts of the bank,” said the firm’s head of mobile.

More broadly, firms reported using constant checks of preventive methods to ensure security of mobile devices, as well as ‘hard blocks’ that can block certain behaviours on the phone.

Storage and retention of captured data also posed a challenge for respondents, particularly given the need for speed and accuracy, and regulatory expectations of ease of access and immutability. Financial institutions are largely familiar with the concept of capturing trading room conversations from sophisticated turret systems. But voice-based trading can now be conducted across many platforms, including turrets, mobile, Skype, conferencing, and IM – aside from trading handled through electronic communications like SMS – making it more of a challenge than ever to capture trading communications and store it in a consistent way.

Where in the past, much of the monitoring of trading conversations was designed to protect the firm in the event of a dispute or misunderstanding, MiFID II requires firms to take an active approach to monitoring and surveillance, as well as putting in place a governance policy to ensure things are happening appropriately.

As a result, firms are looking at surveillance tools, analytics, word spotting and transcribing to perform the analysis they require to meet their regulatory obligations. Getting analytics to work with mobile devices can be much more challenging than applying analytics in a call centre environment. One issue here is the quality of sound and the clarity of speech of those being recorded. This can extend to whether the system can deal with local accents and lexicon/vocabulary.

**Interpretation is the Real Difficulty**

This can lead to difficulties in analysing the recording files. The head of trade surveillance at a Tier 1 European bank said that although his institution was 70% prepared for MiFID II’s requirements in this area, “interpretation is the real difficulty. There is significant loss of fidelity in recordings, and this makes it difficult to interpret the content of the call.” His bank was able to record and store all voice messaging related to trading, but compression of the files result in loss of fidelity, making analysis difficult.
Retrievability is key to meeting the new requirements. One approach is to store all required data in a single repository or data lake, overlaid with search capabilities to allow ad hoc retrieval in response to regulatory requests. But this is not a trivial exercise, and requires consistent indexing of recorded data to transactions, linking together voice messages, SMS, IM, Skype and all other affected channels.

Taking the Mobile Management Policy Route

After the introduction of mobile recording in the UK – under the FCA’s COB 11.7 – the lack of time and robust seamless market solutions forced many firms to ‘manage by policy’ instructing their regulated users not to use mobile devices for trading-related business. This was a legitimate strategy because of the narrow scope of the regulation, which required firms only to record conversations that directly related to a transaction.

For many regulated firms, the default policy seems to be that trading-related conversations can only be held on permitted devices, and any such communication should be recorded 24/7 in any jurisdiction. While this would appear to solve the mobile device issue, respondents to the Intelligent Trading Technology survey acknowledged that issues remained, notably around enforcement of the policy.

The extended scope of MiFID II now challenges the legitimacy of a managing by policy approach, by requiring firms to record all conversations that could potentially lead to a transaction. Ostensibly, this requirement could preclude firms from providing their staff with mobile phones or indeed from instigating a BYOD strategy, on the basis that either approach would render the employee available for mobile communication.

Furthermore, it is not possible in a ‘manage by policy’ environment for a regulated employee to ‘advertise’ a non-recorded mobile
number on their business card or email signature. Under MiFID II, a mobile use policy must restrict application use on a recorded device and legislate against circumvention via unrecorded channels such as WhatsApp, WeChat and iMessage.

While acknowledging the technological challenges posed by meeting MiFID II’s mobile challenges, many respondents to the Intelligent Trading Technology survey relied on the mobile management policies they had in place. Respondents frequently cited their mobile policy when addressing questions of how to deal with issues such as usage of communications apps like WhatsApp or the industry’s growing tendency toward a BYOD approach to mobile use.

Practitioners adopting a ‘manage by policy’ strategy to mobile-based trading-related activity understand that regulators will check that they can demonstrate a robust governance structure and can prove how they’re implementing the policy. Among these practitioners, the default policy seems to be that trading-related conversations can only be held on permitted devices, and any such communication should be recorded 24/7 in any jurisdiction. While this would appear to solve the mobile device issue, respondents acknowledged that issues remained, notably around enforcement of the policy.

This issue is compounded by the fact that MiFID II will switch the burden of proof of mobile compliance to the financial institution, which now needs to prove innocence rather than regulators having to prove the institution guilty. This means firms need not only to come up with data when regulators request it but also need to demonstrate staff understanding of and adherence to mobile policy.

As a result, survey respondents were keen to drive behavioural change in their organisations so as to avoid falling foul of regulators in the first place. As one respondent at a Tier 1 buy-side institution put it: “We need more rigorous policy enforcement. We need to be able to demonstrate that we adhere to policy, and therefore we need records to prove that we do.”

Firms’ position on fully encrypted messaging apps like WhatsApp and Apple iMessaging underscored the issues with adopting a manage by policy approach. Compliance and other managers responsible for enforcing mobile policy need to be aware that these kinds of end-to-end encrypted apps are very difficult and sometimes impossible to record.
Enforcement Challenges

Several respondents said their policy prohibited their use but acknowledged that it was difficult to enforce this restriction. Indeed, respondents said they had heard of instances where major financial institutions had to backtrack on their WhatsApp ban after discovering that senior executives were major users of the platform.

The WhatsApp example points to the challenge posed by the trend toward ‘bring your own device.’ Firms have in recent years eschewed the ‘corporate’ mobile device in favour of a BYOD policy. This has happened for a variety of reasons, among them the demise of the BlackBerry as a kind of corporate phone standard, demand from staff for new smartphone functionality, and simple cost considerations from eliminating hardware costs.

But BYOD – where an employee brings his or her own device and SIM card for work business, whether or not the cost is expensed back to the company – poses challenges with respect to compliance with MiFID II and other regulations governing mobile use for trading-related business. Clearly, if the BYOD device is being used for trading business, it needs to be recorded. But if it’s also being used for personal business, survey respondents said, then recording it verbatim raises privacy issues, particularly as the EU’s new Global Data Protection Regulation (GDPR) comes into force in the spring of 2018.

The solution for many was a blanket ban on BYOD usage for regulated business use. This, however, once again points back to the challenge of enforcement, and under the new regulatory regime firms are unlikely to be able to hide behind the blanket of BYOD, particularly as staff list their BYOD device numbers on their business cards.

One possible solution is to provide a specific app for regulated business on the BYOD device. Again, ensuring the staff member uses this app for specified business is a challenge.

“Business is allowed to use Skype for Business,” said a trade surveillance manager at a Tier 1 UK-based sell-side institution. “But other than that, all other apps are banned by our policies. We provide a list of what they can use; if it’s not on the list, they can’t use it.” But this executive concedes there are conflicts between what’s on the list and what compliance would approve for use by traders, and this is an issue that needs to be revisited.
Instituting Robust Governance

Notwithstanding a firm’s stance on BYOD and unrecordable communications channels, a robust governance programme – in the form of a Mobile Device Management (MDM) platforms – is essential for setting policy and demonstrating adherence to it by affected staff. Policies can be set forth in the hiring process, supported by employment contracts as appropriate. But alongside that, staff need specific education on what the policy means for their work function as well as regular training to ensure they keep these considerations to the fore of their thinking.

Survey respondents emphasized the importance of policy and governance of that policy, but suggested enforcement could be challenging, particularly where specific restrictions on usage of devices or apps was concerned.

One of our biggest concerns is “that BYOD devices are used for illegitimate [purposes],” said a senior compliance manager at a UK brokerage. “Staff are allowed only one phone and there has to be a level of trust that people will comply with policies. This is always a risk, and to avoid it we would have to record everything, but that raises privacy

MiFID II strengthens the corporate governance themes relating to recording trading communications, placing more emphasis on the compliance function. Problems can arise where the view or actions of senior management deviates from the assessment and recommendations of a compliance officer, and any such situation needs to be documented – as the European Securities Markets Authority has stated in the internal controls and governance provisions of MiFID II.
Guidance from the Top

More important, however, is the need for the business side and the compliance function to move closely together to ensure regulatory obligations are met. And once again, the onus is on management to better understand the systems and equipment used by staff so that all devices meet the requirements of the regulation. Certainly, the new record-keeping requirement (as mentioned above) reflects this new onus on proactive management and enforcement of mobile policies.

The result, inevitably, is a trade-off between any restrictions of the mobile policy and the functionality enjoyed by employees using the equipment. Adding too many restrictions, on functions such as texting and communications apps, as well as ownership and responsibility for a device, can negate whatever utility and value smartphones can have for a firm by allowing users to conduct business from anywhere. Worse, by restricting mobile use in order to quickly and easily achieve compliance, firms may find themselves at a competitive disadvantage to rivals who elect not to take such a strict ‘manage by policy’ approach.

Furthermore, the more onerous the policy’s restrictions, the greater the likelihood that policy will be circumvented in some way or, worse, ignored. This was acknowledged as an ongoing issue by survey respondents. Most said their organisations erred on the side of caution, banning the use of BYOD among regulated employees. Others, however, tried to find a balance.

“We recognise there are issues of policy vs. business use vs. the ability to record as appropriate,” said a senior European compliance manager at a major investment firm. “We need to know what we need to record from other devices that are not dedicated to business use.”

One of our biggest concerns is “that BYOD devices are used for illegitimate [purposes],” said a senior compliance manager at a UK brokerage. “Staff are allowed only one phone and there has to be a level of trust that people will comply with policies. This is always a risk, and to avoid it we would have to record everything, but that raises privacy issues.” As mentioned, any recording of BYOD devices or indeed non-business conversations recorded on corporate phones could place the firm in breach of increasingly onerous privacy rules, including the EU’s wide-ranging GDPR, which takes effect in May 2018.

Said another compliance manager at a major buy-side institution: “We restrict use, lock down certain types of services for business use
because of regulation. It’s relatively easy to lock down corporate devices, but can you lock down BYOD devices if they are for personal use? This gets back to the policy of not using devices for inappropriate purposes and being aware that certain investment-related subjects must comply with regulatory provisions.”

**Formal Approach Needed**

Finally, a respondent from another UK buy-side firm said, “There may be a user awareness of risk, but we must manage that and we need to manage usage of applications and services [on BYOD devices]. People are pulled into these situations [using non-approved apps] and don’t know what to do. We have an ad hoc response and need a more formal approach. We may have to ban these apps and services in certain instances, and in others engage and then withdraw if necessary.”

Ironically, regulated individuals operating in the trading and investment environment largely want to comply with whatever policies govern their use of mobile devices. Recording of business phone conversations is nothing new, and few traders object. Several traders and trading operations staff spoken to for this report indicated that they would prefer to communicate as freely as possible in order to conduct business in the safest and most effective way.
Although the requirement for recording trading-related communications on mobile devices traverses several areas of MiFID II’s provisions on surveillance, as outlined above, financial institutions are required to establish for themselves the approach to compliance that best fits their activities and capabilities. While the application of the requirement to firms’ businesses may be highly nuanced, the decision boils down to a series of steps, the first of which seems relatively straightforward: The firm needs to decide between managing by policy or recording everything.

Managing by Policy

Simply put, managing by policy involves prohibiting use of unapproved (unrecorded) devices any communication that may potentially lead to a transaction. This approach was widely adopted when the UK’s Financial Services Authority (FSA), now the (FCA), introduced the requirement for recording of mobile phone conversations: the typical response was to prohibit the use of mobiles for making transactions.

But the scope of mobile phone use within financial services organisations has grown exponentially since then, and MiFID II’s coverage of any communication that could pertain to a transaction (rather than directly resulting in one) means that many firms seeking to apply this rule may be facing a blanket ban on mobile phone use for any business. For most, this is not a practical solution.

Implementing restrictions instead, as we’ve seen from the survey responses, can be difficult to enforce. BYOD certainly presents a number of challenges, and regulators will be looking for evidence that firms have in place a robust governance structure to avoid possible policy breaches, such as listing of executives’ BYOD devices on their business cards or email signatures.

Recording Everything

Given the challenges of managing by policy in today’s complex environment, many firms are looking to take the alternative route of recording all mobile communications generated by regulated staff. Here, firms need to pick an option: whether to use a device-based recording app or in-network recording.

Once again, when the FSA introduced mobile recording in 2011, the vast majority of regulated entities opted to use an app to record mobile communications. Part of the reason for this was that an
The app-based approach can be deployed independently of the mobile network operator, allowing the firm’s IT department to control the whole recording process. This is particularly appealing when it comes to international operations, as it avoids having to deal with unknown suppliers and local regulations.

Today, though, only a small minority continue to use an app, with most having switched to network recording, according to Truphone, which provides in-network recording for nine of the world’s 12 largest investment banks. One reason for this is that a single app is difficult to deploy across a range of operating systems while maintaining consistency of experience and outcome. IT departments are faced with having to deal with BlackBerry, Android, Apple and Microsoft environments, which can present a major challenge.

Finally, an app can degrade the user experience substantially. For one thing, connecting with the recording device can introduce delays. It also introduces an additional point of potential connection failure, which can interrupt time-sensitive conversations. These factors can lead to users circumventing the app, clearly making recording of all communications impossible.

Some firms are attempting to change behaviours by offering incentives for staff to use the recording app, for example by using voice-to-text applications to capture voice communications in CRM systems and alleviate the need for employees to write up notes.

In-Network Recording

Notwithstanding these efforts, however, firms are concluding that in-network recording offers the greatest chance of avoiding a policy breach and resultant regulatory censure. In part, this is due to the fact that in-network solutions are largely invisible to the user and don’t encourage circumvention. There is no delay to the communication and as a result, the user experience is not compromised.

But an in-network solution is by definition operator-dependent, which makes it difficult to manage recording for staff who travel between different roaming environments. Typically, firms that operate across multiple geographies and mobile operator environments will need to establish arrangements with multiple suppliers in order to assure complete recording integrity.
MiFID II raises the bar on mobile voice and SMS surveillance and recording. Financial institutions need to understand how they are impacted, and move swiftly to implement a suitable platform to ensure compliance by the deadline of January 3, 2018.

Firms need to adopt an approach that meets the regulatory requirements, but doesn’t compromise functionality and competitiveness like a blanket ‘manage by policy’ strategy does.

Regulated entities must identify and implement a mobile device management (MDM) platform that meets their usage criteria, meets MiFID II’s recording and storage requirements, and provides the functionality and flexibility needed to retain business competitiveness.

For many firms, these pre-requisites point to the need for an in-network mobile device management approach.
INTRODUCING TRUPHONE

Truphone is the market-leading mobile recording service that helps financial organisations comply with industry regulation, such as MiFID II. Global by design, Truphone Mobile Recording securely captures and stores all voice and SMS traffic seamlessly within the network.

No apps. No delays. No change to user experience. Our global solution is simple to deploy with a choice of on-site or hosted solutions. It’s device and operating system agnostic, delivering a more reliable user experience at home or abroad.

With Truphone, your organisation benefits from having a single supplier to deliver a fully compliant global recording solution, mobile service and customer support – avoiding the complexities of multi-vendor relationships.

Speak to us today:
Paul Liesching, Head Of Global Financial Markets,
Paul.Liesching@truphone.com
www.truphone.com/uk/mobile-recording
A-TEAM GROUP

A-Team Group provides news and analysis, white papers, webinars, events and more through our two online communities:

- Intelligent Trading Technology
  www.intelligenttradingtechnology.com
- Data Management Review
  www.datamanagementreview.com


Sign up as a member free, download recent white papers, or look at our upcoming webinars and events and book your place today.

If you’re a vendor and looking for high quality content – like this white paper – to help articulate your message, take a look at www.a-teamgroup.com.

Or get in touch: 020 8090 2055 / theteam@a-teamgroup.com.