Operational Risk & Regulation

Criminal minds and increased surveillance

By Mark Sands

Recent high-profile convictions mark success for regulators' increased market surveillance efforts, and this greater emphasis on oversight means firms are having to reassess their own monitoring systems

The recent conviction of Raj Rajaratnam, the founder of hedge fund Galleon Group, has highlighted regulators' increasing focus on criminal activity in the markets. Rajaratnam's verdict is a victory for the US authorities not only because of the size of his crimes, but also because of the prominence the case has achieved, with the market surveillance methods and potential penalties discussed at length.

"Since the Galleon case was first brought by this office, our prosecutions have been responsible for dismantling elaborate networks of corrupt executives who gamed the system, exploited their access to proprietary information, shirked their ethical responsibilities and violated the law with impunity," said Preet Bharara, US attorney for the southern district of New York. "We will continue to work tirelessly with our partners at the FBI to root out corporate corruption on Wall Street and to hold privileged professionals who gallop over the line accountable for their actions."

The UK Financial Services Authority (FSA) has also achieved a smaller-scale success in recent months, with the conviction in February of Christian Littlewood, formerly of Dresdner Kleinwort, for insider trading – the first time a banker has been charged with insider trading by the FSA while still in their job.

The main priorities for regulators in market surveillance are detecting and stopping insider dealing and market manipulation, while also making sure that customers are treated fairly – and it is clear that for the first two at least violations will be met with serious penalties. At the time of going to print, Rajaratnam's sentencing had yet to occur, but Littlewood was sentenced to 40 months' imprisonment, the longest sentence yet handed out for insider dealing in the UK. His co-conspirators received similarly stiff sentences.

At the time, Margaret Cole, the FSA's managing director of enforcement and financial crime, commented: "A tough, co-ordinated approach to insider dealing and our commitment to taking on difficult criminal prosecutions has really begun to pay off."

In the US, the Securities and Exchange Commission (SEC) has launched seven insider-dealing investigations this year, most recently against former managing director of Nasdaq Donald Johnson, who pled guilty to securities fraud. Johnson faces up to 20 years' imprisonment and a fine that could go as high as $5 million. In reference to Johnson's prosecution, assistant attorney-general Lanny Breur said: "Insider trading by a gatekeeper on a securities exchange is a shocking abuse of trust, and must be punished. The integrity of our securities markets is vital to the US economy, and the Justice Department is determined to take on insider trading at every level."

Such intense regulatory scrutiny should not only raise alarm for potential wrongdoers, but also be worrying for those in charge of internal compliance and market surveillance networks, whose lapses could be similarly punished.

"In Germany a compliance officer [in a transport company] last year was recently sentenced," says Wolfgang Fabisch, founder and chief executive of German compliance solution provider b-next. "He was found guilty of not putting the right processes in place in his organisation. He was not the one who stole the money, but he left the door open. Compliance officers were upset because they realised they could be found guilty if their processes are not in line. That was new to them."

Bill Nosal, senior managing director at NasdaqOMX – Smarts, a surveillance technology provider, agrees. "The regulators have been clear there is an expectation firms monitor their trading activity, and that

expectation goes back a long time," he says. "The firms themselves recognise self-reporting can be a mitigating factor in any potential settlement on a regulatory violation, so most want to monitor actively for potential violations and self-report, rather than get surprised by a regulatory inquiry they know nothing about."

He notes that the penalties both to the individual and the firm for the alternative can be severe. "Organisations such as the Commodities and Futures Trading Commission (CFTC) could bring charges that amount to huge penalties, millions of dollars per day per violation," he says. "In certain markets, these levels of penalties are really putting a lot more fear into firms."

Nosal cites the flexing of the CFTC's muscles as a driving factor behind the compliance efforts of firms that trade in the energy and commodity market, and says firms should note the level of co-operation between regulatory entities such as the CFTC, the Federal Energy Regulatory Commission and the UK's FSA. "The regulatory bodies are sharing information to help make it easier to prove intent in cases around market manipulation and market abuse – this could lead to much more severe penalties than traders and firms in these markets have experienced to date," he says.

Even when alleged insider dealers manage to avoid jail, Nosal argues, the fact they have been dragged into court should send a strong message to others. "The huge legal costs associated with staying out of jail and/or avoiding fines coupled with the reputational impact to the firm or individual is a strong deterrent," he says.

And there are probably more charges to come – the investigation into Rajaratnam and Galleon began in 2008 and, similarly, the UK FSA spent two years building its case against Littlewood.

"When you look at the news today and you see settlements against various firms; many of those settlements are on cases that were brought back in 2007 or 2008, maybe now the 2009 timeframe," says Nosal. "We are probably only seeing the tip of the iceberg of the cases that are going to be brought forward for some of these manipulative and other types of behaviours. The regulators' mandates, and sometimes their budgets, are expanding, the examinations are getting much more rigorous, and the expectations on firms are increasing. You can bet there's going to be more of these cases, and it seems likely the penalties will climb to much higher levels."

In the past, regulators took a more simplistic approach to analysing a firm's ability to survey the market and ensuring compliance. But Nosal says this has shifted, and authorities now possess a much keener eye for what market surveillance entails.

"When the regulators came in for an exam, it used to be adequate to just show them your automated surveillance tool, and you generally got the check mark for having an adequate approach to trade monitoring," he says. "But today, the regulatory examiners have higher expectations and ask harder questions. They're drilling down into the applications themselves, and expect firms to show them how the detections work for each behaviour they are monitoring and each alert they are generating. And they're also asking about what the firm is not doing."

"It's clear staff numbers have been beefed up, and processes and procedures have been beefed up, over the past few years," agrees Michael Markov, founder and chief executive of quantitative analytics provider Markov Processes International (MPI) in New Jersey. "I don't want to speculate whether this is the result of improved procedures on the part of the US SEC or other regulatory bodies, or just a surge in illegal activity. There's clearly a relationship with both, but as we all know, correlation does not mean causation. One would hope this is happening because governments have started investing more in surveillance, but there is a limit on what they can do with existing technology. If it's wire-tapping, for example, you can't wire-tap the entire market."

“Twenty years ago in Germany, a law came out regarding ‘market conformity’, which meant that as a market participant you needed to make sure every single transaction you did was aligned with the market,” says Fabisch. “To do that, you need technology that will get every single transaction and compare that to a market. It sounds simple, but it’s very complex because you’re doing hundreds of thousands or millions of transactions across multiple markets.”

There are obvious challenges with parsing of such data – sheer quantity is a problem – but Fabisch says it is vital to make sure every transaction is observed.

“We take the approach that to understand the business you need to look at all the complex patterns and interactions across all the asset classes,” he says. “You need to see what’s going on over time and have the management information to give you the top-level view. You must look at every single transaction to determine what’s going on.”

However, he notes few financial criminals will trade directly on companies about whom they have inside information, but will have more advanced methods of disguising their activity.

“If you employ stupid people and they get knowledge of inside information – on British Airways, for example – they’ll buy or sell BA because they know what’s going to happen,” says Fabisch. “But if you are working with more sophisticated people, they will do derivatives because the leverage is much higher. And if they’re a bit more sophisticated, they will buy derivatives where BA is only the underlyer – the derivative is in UBS or RBS products. So you as a compliance officer are looking for BA but you will not find it.”

As a result, compliance officers who are already examining large swathes of data are finding their pools continue to expand as related companies and possible underlyers are added to watch lists. “If you put BA on your watch list, I’m quite sure you would have to add to your watch list another 150 or 250 pages related to BA,” he says. “If you have 20 companies on your watch list, that means you have to look at 4,000 items, and if someone in your business does 4 million transactions a day... You can’t do that.”

This pressure is also falling on regulators, who are keen to see their markets attract further business, argues Fabisch.

“If investors lose trust in the industry or in one place where the industry is important, such as London, they will quickly shift their money to other places where they can better trust what is going on, and where they are handled fairly,” he says. “The pressure is on the regulator to make sure the market is fair, and operates in a fair way, because otherwise investors are going to say: ‘I don’t want to put more money in.’” Smarts offers surveillance tools to exchanges, regulators and broker-dealers, and while these take the form of two different products, Nosal says there is a overlap in the behaviours of interest. “At the base level, the behaviours you are looking for in market manipulation are common across the two products,” he says. “The details of how each regulator or exchange wants to do it typically requires a greater degree of customisation. Meanwhile, the approach the broker-dealers take can be standardised, while always ensuring each firm using the solution is able to set parameters for alert generation that match their unique trading activity and compliance philosophy. So you can expect a behaviour like wash trades – a straightforward alert – to be available in both applications.”

Nosal says he has observed a shift in attitude in the markets and more substantial surveillance techniques are being applied, even in the equity markets, where automated solutions have been widely implemented. “It’s been an equity-centric world from a surveillance perspective for a long time, and while most firms have some solution, that doesn’t mean they have an adequate solution to meet today’s regulatory expectations,” he says.

Perhaps the biggest shift is surveillance is happening at the asset class level. “The role of regulators, coupled with all the things that are happening through regulations such as the Dodd-Frank Act and the Markets in Financial Instruments Directive, are really extending the demand for surveillance on other types of asset classes. That means asset classes like derivatives and fixed income, including vanilla bond products, interest rates swaps and credit default swaps, along with energy and commodity instruments traded on-exchange and over the counter can benefit from automated surveillance capabilities. The circle is just getting bigger and bigger in terms of what firms need to survey.”

Regulators now expect the best practices of market surveillance in the equity space should be applied to other asset classes, and Nosal argues this is starting to cause a redistribution of compliance and surveillance staff.

“We’re seeing firms pulling experienced surveillance people from their equity surveillance groups, and bringing in them into other asset classes – applying that best-practices mentality,” he says. “They’re saying: ‘Here’s how we did it over here in these highly-regulated cash equities markets, and we’re going to start looking at similar or related behaviours against your derivatives trading, against your fixed-income trading, against your swap trading, all of those kinds of things.’ That’s a big shift.”

The growing volume of data, however, continues to pose challenges and firms are only able to keep pace by investing in substantial technological infrastructures. “Now you’ve got a situation where the regulators are saying: ‘Well, now you need to look at your derivatives as well as your equities, I want you to look at your over-the-counter trades and I want you to look at what’s going on with fixed income.’ I don’t think you’re going to be able to do that with typical existing compliance resources and without technology,” says Fabisch.

Such systems can raise problems of their own, with firms employing either easily exploited systems, or ones whose flaws are known because they have been designed in-house. There needs to be an external validation of those systems, he says. “If you know the back door, then you’re also exposed. Or if it’s built internally on Excel or Access, and then the person who built the system goes to another organisation, serious risks are being run.”

With the price of such systems proving another hurdle for compliance departments, it’s vital firms are able to get buy-in from the top, something Fabisch argues will be aided by the increased regulatory scrutiny and prominence of recent convictions. “One of the benefits of this increased market and regulatory scrutiny and oversight is that practitioners are now able to go to their management teams and say, ‘Hey, the FSA is coming, they want to see more reports on insider dealing or market abuse, and I don’t have the tools or the people to look at this,’” he says.

In the past, there have been examples of trading desks being far better equipped than their counterparts in compliance, leading to a fundamental mismatch. Fabisch hopes this will be rectified by such cultural shifts. “It’s within the power of senior management to recognise that the risk and compliance department needs to be as well equipped as the trading organisation, and to make sure they’re well balanced. If there’s a mismatch, how can they be sure the returns they’re making aren’t built on sand – that the returns they’re getting are real returns versus a Kerviel or a Galleon?”

These challenges are not just internal. Firms must observe their own staff, but many also survey their counterparties, in part for reasons of stability, something that Markov at MPI advocates.

“We are known in the industry for pioneering forensic returns-based due diligence – it was called returns-based analysis back in the early 1990s,” he says. “The idea is to take the performance of an investment portfolio or product and mimic it with indexes to do performance due diligence – to understand what the manager does without knowing positions, having no insight into their workings, but just using performance numbers.”

Operational Risk & Regulation

While many surveillance solutions begin by looking at all the individual trades executed by a firm or broker, Markov advocates doing the reverse, and starting at the results of a firm in what he calls a top-down approach. Although he describes it as a due diligence approach, he notes the method also has surveillance applications.

“That same technology with a different twist, with certain improvements, can be used for applications in the surveillance segment, looking for excessive leverage, or maybe looking for potential frauds, for red flags, understanding the complex products that are hard to explain,” he says.

This method allows firms to effectively deduce strategies at other firms and avoid potential counterparty risks, without being forced to wade through information, which Markov says can be counterproductive. “The more data you have, the more issues you have,” he says. “Exchanges and government oversight bodies look at trades and improprieties of trades – it’s a vast amount of data. It’s one way of looking at things, but we look at things from a different angle. They take a bottom-up approach and we look from the top.”

“The issue is that you can miss certain things. It’s just a lot of data; you might just not make it down through all of the various different channels, so it might not even alert you at all,” says Markov.

Regardless of the methodology employed, Fabisch argues greater scrutiny can only be a good thing. If regulatory actions create more stable, profitable and reputable markets, every participant will win, he says. First, however, the industry must move forward. “The industry is understanding step by step that it’s not only a problem for the regulators and for the public, but that firms have to clean up their own houses. They have vital interests to make their processes more secure, not to be open to fraudulent actions,” says Fabisch.

“They have to understand and optimise their processes, they have to reduce operational risk. Maybe one day there will be a monument to Jérôme Kerviel, because he did a lot to get banks, investors and regulators to see this as a top priority.”

http://www.risk.net/operational-risk-and-regulation/news/2078136/criminal-minds-increased-surveillance/