Global investigations: reading the signals

As the global economy recovers, how will regulators respond? Experts provide perspectives on trends in regulatory and corporate investigations.
Global trends in regulation

In the wake of the financial crisis, there has been a sustained rise in the number and variety of investigations and enforcement actions taken by regulatory authorities globally. Multinational corporations and financial institutions are now more likely than ever before to find themselves subject to cross-border investigations conducted in parallel by multiple authorities.

Regulatory authorities around the world are continuing to investigate and prosecute business conduct aggressively and to impose record-setting penalties in the process. There is no sign that this trend will abate. Quite the contrary. And, while US authorities remain in the vanguard of such initiatives, now more than ever non-US authorities can be expected not only to cooperate with and facilitate US enforcement initiatives, but also to pursue their own criminal or regulatory investigations and to exact their own significant penalties. This trend of global scrutiny toward and enforcement against certain business conduct is facilitated by the broad jurisdiction of anticorruption laws such as the US Foreign Corrupt Practices Act and the UK Bribery Act as well as various antitrust, sanctions and anti-money laundering regimes. Enforcement authorities, particularly in the United States, have used such laws and accompanying legal doctrines to prosecute corporate and individual misconduct in far-flung markets that may have little apparent nexus, for example, to the United States.

For this report, we invited a number of experts to provide different perspectives on this changing regulatory landscape and what it means for business. The articles consider what the current challenges are, how things might develop in the future, and what the implications are for financial institutions, corporates and their officers, directors and employees around the globe. We also look at the US and EU sanctions levied as a result of the crisis in Ukraine.

We hope that you enjoy this report, and we welcome the opportunity to discuss these subjects with you in greater depth.
In no uncertain terms

Regulatory uncertainty rather than complexity is the biggest challenge facing general counsel of multinationals

François Garnier
Chief Counsel International Platform, Pfizer

Uncertainty can be the biggest regulatory challenge facing the general counsel of multinational companies. Give me enough certainty—clear rules and guidance—and I can structure my operations. But when regulations are unclear or unstable, it can be almost impossible to develop reliable compliance or business strategies. As the Chief Counsel International Platform at Pfizer, I’m familiar with the challenges posed by regulatory complexity. The pharmaceutical industry is highly regulated, and Pfizer has operations in every major trading country around the globe. Each of these countries has its own regulatory framework that can include complex and multi-layered systems of controls. Regions within countries may also be subject to different regulations. And antitrust and anticorruption laws—such as the US Foreign Corrupt Practices Act and the UK Bribery Act—have extraterritorial jurisdiction and thus apply to virtually every company trading internationally.

We have to ensure that we’re doing the right things at the regional, national and global levels. And we have to be as vigilant with partners as we are with ourselves—vendors and providers must undergo the same checks and controls that we apply internally, and they must understand that Pfizer has zero tolerance for non-compliance.

It’s possible to overdo it. Excessive controls can slow business down and stifle innovation. It is important to find the right balance. But uncertainty is a bigger problem still. As long as I know what is required of me, I can deal with even the most stringent requirements. It may be costly, introducing complex and excessive bureaucracy to the company, but these challenges are manageable—and they pale in comparison to uncertainty.

Emerging markets pose the greatest challenges. Regulations in these countries can be ambiguous, and guidance from rule makers can be vague or non-existent. Even worse, regulations may change frequently and unexpectedly in these countries, leaving companies unsure how long their compliance strategies will be effective or relevant.

Separation of powers and due process are critical in the regulatory context, as elsewhere. Authorities have the power to grant market access and regulate operations, but in many jurisdictions they also act as police and judge. I would like to see a better balance of power between the regulator and industry, but in many cases this will depend on the local judicial authority.

There’s reason to believe that regulatory activity will increase across industries and countries in the foreseeable future. If that happens, regulations will play an increasing role in setting competitive conditions and determining opportunities for growth. In such an environment, the need for clarity and consistency is all the more important. Regulatory uncertainty not only makes it difficult for companies to do business, it reduces their ability to comply. That’s a loss for businesses, regulators and society in general.

Scoring a common goal: cooperation between agencies

Antitrust agencies are waking up to the idea that fighting bribery is essential to the maintenance of competitive markets

David Vascott
Editor, Global Investigations Review

It might seem obvious that corruption hurts competition. Yet historically, anticompetitive and anticorruption agencies in most countries rarely work together. That may be about to change. Discussions at the Organisation for Economic Co-operation and Development (OECD) 2014 Forum on competition suggest that antitrust agencies increasingly recognize that they need to play the part in eradicating corruption. Several speakers called for greater cooperation with their anticorruption counterparts—emphasizing, for example, that it is impossible to maintain competitive markets unless bribery laws are enforced.

Obiageli Ezekwesili, co-founder of Transparency International, an anticorruption organization, summed up the emerging consensus: “Everything that corruption likes, competition dislikes,” she said. “Competition wants to do things in a clandestine environment, but…the more transparency, the greater the competition. Corruption wants to hide things in a clandestine environment, but…the more transparency, the greater the competition. Corruption doesn’t care for value for money, but competition is about value. Corruption doesn’t care about the interests of the greater majority, but competition cares about the interests of the greater majority.”

The Forum, which is held every year at the OECD’s Paris headquarters, convenes national representatives from competition agencies around the world. As such, the event is a bellwether for developments in the field. The root of the problem is the fact that agencies often do not share information, even when doing so would enable them to achieve common objectives. Most antitrust agencies carry out dawn raids to investigate antitrust violations. Information discovered during their investigations could often be evidence of corruption, but antitrust investigators may not be trained to recognize it as such. In addition, it may be difficult to share findings across agencies for both institutional reasons and other factors such as different standards of evidence gathering. It is unlikely that we will see mergers between antitrust and anticorruption agencies due to the institutional and legal obstacles that would need to be overcome. However, the recent signing of a memorandum of understanding between the UK’s Serious Fraud Office and the Competition Markets Authority detailing mutual cooperation in criminal cartel proceedings may be a sign of things to come. Greater cooperation—from gathering evidence and sharing information to extending cartel leniency agreements to cover corruption issues—may be both desirable and achievable for authorities.

This could have significant implications for business. If competition enforcers carrying out a dawn raid are also on the lookout for potential corruption issues in the target company, that company’s counsel may find they have an entirely new front to defend—one that potentially ramiﬁes far beyond the immediate antitrust issue. With the extraterritorial reach of the US Foreign Corrupt Practices Act, the UK Bribery Act and other far-reaching national bribery laws, an investigation launched on the back of a domestic antitrust issue could quite feasibly open up a Pandora’s box of cross-border, anticompliance problems.
The inexorable rise of EU fines

Tough EU financial penalties alone may not be acting as an effective deterrent to anticompetitive behavior, and are instead having other unwelcome impacts. The European Union last year handed down record fines for anticompetitive behavior totalling €1.9 billion or $2.3 billion. That’s more than double the fines imposed by antitrust authorities in the United States and ten times more than those in China.

In the last five years, the EU has imposed antitrust fines of more than €8.6 billion in ever-increasing amounts and has the ability to levy fines of up to ten per cent of a company’s—or its group’s—annual global turnover. This year looks set to be another bumper year with ongoing probes into the auto parts industry, among others.

The scope and targeting of the EU’s fining policy is also being expanded. This year, for the first time, a private equity fund was fined just over €37 million by virtue of its controlling stake of a suspected cartelist in the power cables case, without there being any evidence that it was aware of any infringement.

In what is a clear warning to private equity firms, European Commissioner for Competition Joaquín Almunia highlighted “the responsibility of groups of companies up to the highest level of the corporate structure to make sure that they fully comply with competition rules.” “These responsibilities are the same for investment companies who should take a careful look at the compliance culture of the companies they invest in,” he said. In response to criticism, EU chiefs continually insist their regime of tough financial penalties acts as a deterrent. The bigger the fine, the bigger the deterrent, the story goes. But not everyone is convinced.

In a 2013 paper entitled Antitrust deterrence: The bigger the deterrent, the story goes. Indeed, cartels continue to form, and each year the EU launches a number of new investigations, ultimately imposing large fines on a number of companies.

“EU authorities have a tendency to use the size of fines as a benchmark to show they are doing a good job,” says James Killick, a competition law partner at White & Case in Brussels. “The underlying idea is that the best way to get people to comply is to fine their companies increasing amounts of money. On top of that, each successive competition commissioner wants to show they are more successful than the previous one, so there is a tendency to increase fines.” “But the outcome is that competition fines are far higher and disproportionate compared with those imposed for other regulatory breaches, such as health & safety, violation of consumer protection rules or major environmental damage, for example,” Boris Kasten, head of competition law at global elevator and escalator group Schindler, agrees. “It’s a race to the top in terms of EU fines, without much reflection on whether this alone, without reflecting companies’ specific compliance systems, really serves as a deterrent,” he says. “There may even be an international trend to impose giant fines on corporations as a sort of competition among enforcement agencies.”

That said, in the United States, which has a long history of antitrust enforcement, fines are much lower due to more sophisticated types of punishment, involving fines and criminal sanctions against the individuals guilty of violations, according to Dr Kasten.

Individuals who fix prices or allocate markets as a way of ensuring business outcomes, for example, which may not actually be in the company’s interest, are subject to criminal sanctions under national law in the United States, the UK and several other EU member states. “A fine of double a manager’s annual earnings or possible incarceration would act as a deterrent,” he says.

Large EU fines on companies also impact economic growth. Research by Oxford Economics shows that the most likely resulting scenario is the company will reduce the amount it spends on investment. This will generally mean fewer jobs are created within that company.

Firms will also purchase fewer inputs from their suppliers who, in turn, will employ fewer people. And these suppliers will themselves purchase less from their own suppliers, and so on, with additional effects on potential employment and household spending. Therefore, a large fine on cartel participants will have a knock-on effect across the economy as a whole.

“EU authorities use the size of fines to show they are doing a good job”

James Killick, Partner, White & Case, Brussels

€8.6bn

Amount of EU antitrust fines in last five years

Source: European Commission

5 Global investigations: reading the signals

James Killick, Partner, White & Case, Brussels
The EU should recognize when companies have done a proper job in trying to get their workforce to respect the rules

Charles Balmain, Partner, White & Case, London

In recent years, the press has been full of reports of non-US companies being investigated and, at times, prosecuted by enforcement authorities in the United States for a host of alleged violations of US law. Individuals, too, have been charged, extradited and gone to jail in the United States, not without first setting foot in the United States during the alleged misconduct. US enforcement authorities are aggressively interpreting and applying US criminal laws to companies and individuals outside the United States, including for conduct with little apparent nexus with the United States. Exposure to potential violations of US law can arise from a number of circumstances, and it is more critical than ever to identify and mitigate those risks. For example, US regulatory and enforcement officials often take the position that the mere transit of emails through the United States - sent from one person outside the United States to another outside the United States - is enough to reach the conduct required under US criminal law. Similarly, US authorities may assert that transit of money through the United States on its way from one non-US location to another non-US location is enough to create US criminal jurisdiction. This application of US criminal law can result in significant fines and penalties, including imprisonment. Given the potentially long reach of US law, non-US companies and individuals should manage their legal risk in advance of any potential issues. One of the best ways to address these risks is regularly undertaking risk assessments to determine where there may be exposure to US laws. Another is to create and implement appropriate compliance policies and procedures to conduct transactions in accordance with all applicable laws. Once appropriate policies and procedures are in place, relevant personnel should be trained on a regular basis, including on changes in the law and emerging risk areas.
How US laws can apply

**MEANS OR INSTRUMENTALITY OF INTERSTATE COMMERCE**

Many US laws—including the Foreign Corrupt Practices Act (FCPA) in certain circumstances and various antifraud statutes—may establish jurisdiction over a crime whenever it involves the use of any “means or instrumentality of interstate or foreign commerce.” The term is broadly defined by US authorities and may cover any communication or movement that crosses state or international borders, including wire transfers, emails, phone calls, mail and travel. Given the reach of US commerce, from free email servers to correspondent banks that clear US dollars for non-US based banks, such a broad definition can significantly increase the reach of US law. Furthermore, according to US authorities, a defendant commission or individual need not use the means or instrumentality of interstate commerce themselves—it may be enough for them to have “caused” the use, such as an instruction being sent to one person, who then forwards it to another, through email servers in the United States.

**CONSPIRACY**

Conspiracy law may subject non-US companies or individuals who have not committed an act within the United States to US criminal jurisdiction. Under long established principles of criminal liability, a conspirator may be liable for a coconspirator’s acts, as well as for any “reasonably foreseeable” offenses committed by a coconspirator. If the United States can establish jurisdiction over a single conspirator, it may have jurisdiction over all conspirators, whether companies or individuals, wherever they may be found. In certain circumstances, a conspirator need not have participated in or even known about the underlying criminal offense committed by a coconspirator to be liable. Moreover, unlike conspiracy law in some other countries, under US criminal law, a company can “conspire” with its employees, so corporate crime in the United States may result in a prosecutable conspiracy.

**AGENT LIABILITY**

A company or an individual also may be prosecuted under some US laws. If the company or an individual is found to have acted as the “agent” of a company or individual that falls under a jurisdictional exception. For example, a Japanese trading company was recently prosecuted for violating the FCPA’s anti-bribery provisions as the “agent” of a US company, even though the trading company did not act within the United States. A company potentially also may be liable for third parties’ actions if those third parties are acting on the company’s behalf and for the company’s benefit. Similarly, under this principle of respondeat superior, a company employee who is acting within the scope of his or her employment, and for the benefit of the company, is considered an agent of the company. If they commit a crime connected to their employment, the company may be criminally liable as well.

**PIERCING THE VEIL**

A company may be liable for another’s conduct under the corporate liability principles of “alter ego” or “piercing the veil.” For example, a parent company may be liable for its subsidiary’s acts if it can be shown that the subsidiary was acting as the “alter ego” or under the control of—the parent. If a subsidiary outside the United States is determined to be an “alter ego” of the parent, US authorities may be able to “pierce the veil” of legal separation between the companies, and, if so, the foreign company’s actions can be treated as if they were committed by the US company. Once an alter ego relationship is shown to exist, either in general or in a specific instance, the subsidiary’s conduct and knowledge may be attributed to the parent.

**FOLLOWING THE MONEY: MONEY LAUNDERING AND SANCTIONS**

US law makes it a criminal offense to engage in or attempt to engage in a financial transaction involving funds that are known to be the proceeds of certain unlawful activities, or to engage in a financial transaction that provides funds for the commission of a crime (such as terrorist financing or sending a bribe payment). This offense is called “money laundering.” Non-US corporations and foreign nationals may be subject to prosecution under US federal anti-money laundering statutes if they are involved in the transfer or attempted transfer of illegally obtained funds or funds used to further criminal activity. Money laundering offenses can be as serious as the underlying offenses they promote. Each financial transaction can be considered a separate offense and is punishable by substantial fines and possible imprisonment. Additionally, funds and other property involved in money laundering may be frozen or seized by US enforcement authorities, or subject to forfeiture, without proof of guilt.

**Transit of money through the United States on the way from one non-US location to another non-US location may be enough to create US criminal jurisdiction**

Money laundering offenses can be as serious as the underlying offenses they promote. Each financial transaction can be considered a separate offense and is punishable by substantial fines and possible imprisonment. Additionally, funds and other property involved in money laundering may be frozen or seized by US enforcement authorities, or subject to forfeiture, without proof of guilt. In prosecuting money laundering offenses, the US Department of Justice takes the position that jurisdiction exists over a financial transaction if the laundering is completely a US citizen anywhere in the world, or by a foreign national or non-US corporation if the criminal conduct occurs in part in the United States—even if the foreign individual or company never themselves took an action in the United States, or intended for an action to occur there. This broad jurisdiction can greatly expand the reach of the US money laundering statute. For example, US corporations and individuals potentially may be prosecuted for money laundering offenses involving financial transactions that occur wholly outside the United States. US courts have held that financial transactions that provide funds for the commission of crimes (such as in antitrust matters, virtually, every dollar denominated transaction potentially is linked to certain sanctions) in US commerce as well as with other nations. While there does need to be an actual US nexus for money laundering laws to apply—the dollars being cleared through a US correspondent bank, for example—and there are dollar-denominated transactions that have no such tie, US enforcement authorities increasingly operate on the assumption (unless convinced otherwise) that they have jurisdiction for such offenses whenever a suspect transaction is denominated in US dollars.

The jurisdiction potentially created by clearing US dollars through a US bank can also significantly extend the reach of US sanctions laws. Sanctions can prohibit or restrict doing business with countries (such as Cuba, Sudan, and Iran) or individuals or companies referred to as “specially designated nationals” or “SDNs,” which are ‘blacklisted’ parties subject to US asset freeze, and entities placed on the “Sectoral Sanctions Identifications List” (SSI List), as in the case of the Ukraine-related sectoral sanctions. Sanctions regimes typically cover all “US persons,” but what qualifies as a US person may change from one sanctions regime to the next, as each set of sanctions varies slightly. Generally, it includes any US citizen or permanent resident and any US company, wherever they are in the world, as well as any person physically in the United States. In addition, in certain instances, sanctions may reach non-US subsidiaries of US companies. This may mean that the clearing of dollars through a US bank—may be enough to create US jurisdiction over such transactions. The location of funds outside the United States does not necessarily mean they are beyond the reach of US enforcement authorities. Under US law, the proceeds of criminal offenses—including some offenses that occur entirely overseas—may be subject to forfeiture and may be frozen and eventually seized by US authorities through transactions initiated in US courts. With a judgment of forfeiture issued by a US court in hand, US authorities may be able to freeze not only funds located in US bank accounts, but also funds deposited in foreign bank accounts in view of the increase in cooperation among and between enforcement authorities in different countries. **$2.210m**

**Energy**

**$882.74m**

**Consulting**

**$313.2m**

**Health**

**$148.1m**

**Infrastructure**

**$225.5m**

**Manufacturing**

**$231.2m**

**Telecommunication**

**$457.09m**

**Defense & Aero**

**$50.8m**

**Agriculture**

**$148.1m**

**Infrastructure**

**$225.5m**

**Manufacturing**

**$231.2m**

**Telecommunication**

**$457.09m**

**Defense & Aero**

**$50.8m**

**Agriculture**
Global investigations legislation & enforcement

Anticorruption legislation
- National legislation with global coverage (FCPA, UK Bribery Act)
- Recent national anticorruption legislation
- No data
- OECD convention signatories
- UNCAC states parties
- UNCAC not signed or ratified
- UNCAC signatories

Impact of anticorruption regulations on company policies & procedures
- No impact
- Minor impact
- Major impact

Increased enforcement of FCPA
- 16%
- 30%
- 53%

Bribery Act 2010
- 14%
- 36%
- 49%

Local/other regulations
- 11%
- 42%
- 45%

Dodd-Frank Act
- 31%
- 41%
- 28%

FACTA
- 34%
- 39%
- 27%

Corporate-cartel fines imposed by the US Department of Justice
- Number (left)
- Amount, US$m (right)

Source: White & Case


Source: 2014 Business Anti-Corruption Portal

Foreign bribery enforcement actions by country

Source: 2014 Business Anti-Corruption Portal

FSA and FCA fines

Source: 2014 Business Anti-Corruption Portal

Criminal anti-trust fines imposed by EU Commission* vs. US Department of Justice

*Not adjusted for Court judgments

Source: 2014 Business Anti-Corruption Portal
Challenging sanctions designations: politics and the judiciary collide

Given the potential impact of political sanctions, it makes sense to ask if there is anything designees can do to challenge the decision to impose sanctions on them. White & Case’s EU and US sanctions teams provide some details about the potential for challenging an asset freeze designation in Europe and the United States.
The EU has jurisdiction in the following five situations:

1. within the EU territory
2. on a board of an aircraft or vessel under EU Member State jurisdiction
3. nationals of EU Member States living outside the EU
4. entities incorporated or constituted under the law of a Member State
5. entities in respect of any business done in whole or in part within the EU

The prohibited party of available legal remedies (i.e., either request that the Council reconsider the listing or challenge the sanctions before the General Court of the EU) may not be available in situations where there may be important security concerns that warrant these secret and swift practices. Fundamental due process rights can also weigh against such sweeping governance authority. Challenges to these listings can therefore be important.

Lately, there has been a string of EU court decisions nullifying EU asset freeze listings, chiefly because listing criteria were not met. For example, a June 2014 court decision annulled the listing of the International Islamic Bank for insufficient grounds, where the listing was based mainly on allegations that the bank had allowed other listed banks (state-owned Commercial Bank of Syria and its subsidiary Syrian Lebanese Commercial Bank) to circumvent EU sanctions by facilitating transactions for their (non-listed) account holders. A series of judgments arising from challenges to the EU listing of Mr. Yassin Abdulrahman Kadi – listed by the UN Sanctions Committee based on concerns that warrant these secret and swift practices, fundamental due process rights can also weigh against such sweeping governance authority. Challenges to these listings can therefore be important.

Lately, there has been a string of EU court decisions nullifying EU asset freeze listings, chiefly because listing criteria were not met. For example, a June 2014 court decision annulled the listing of the International Islamic Bank for insufficient grounds, where the listing was based mainly on allegations that the bank had allowed other listed banks (state-owned Commercial Bank of Syria and its subsidiary Syrian Lebanese Commercial Bank) to circumvent EU sanctions by facilitating transactions for their (non-listed) account holders. A series of judgments arising from challenges to the EU listing of Mr. Yassin Abdulrahman Kadi – listed by the UN Sanctions Committee based on concerns that warrant these secret and swift practices, fundamental due process rights can also weigh against such sweeping governance authority. Challenges to these listings can therefore be important.

Lately, there has been a string of EU court decisions nullifying EU asset freeze listings, chiefly because listing criteria were not met. For example, a June 2014 court decision annulled the listing of the International Islamic Bank for insufficient grounds, where the listing was based mainly on allegations that the bank had allowed other listed banks (state-owned Commercial Bank of Syria and its subsidiary Syrian Lebanese Commercial Bank) to circumvent EU sanctions by facilitating transactions for their (non-listed) account holders. A series of judgments arising from challenges to the EU listing of Mr. Yassin Abdulrahman Kadi – listed by the UN Sanctions Committee based on concerns that warrant these secret and swift practices, fundamental due process rights can also weigh against such sweeping governance authority. Challenges to these listings can therefore be important.

Lately, there has been a string of EU court decisions nullifying EU asset freeze listings, chiefly because listing criteria were not met. For example, a June 2014 court decision annulled the listing of the International Islamic Bank for insufficient grounds, where the listing was based mainly on allegations that the bank had allowed other listed banks (state-owned Commercial Bank of Syria and its subsidiary Syrian Lebanese Commercial Bank) to circumvent EU sanctions by facilitating transactions for their (non-listed) account holders. A series of judgments arising from challenges to the EU listing of Mr. Yassin Abdulrahman Kadi – listed by the UN Sanctions Committee based on concerns that warrant these secret and swift practices, fundamental due process rights can also weigh against such sweeping governance authority. Challenges to these listings can therefore be important.
Sanctions and export controls can hit hard and fast

International crises, most recently in Ukraine, Syria and Iran, have resulted in large US-led sanctions imposed against “offending” states—requiring businesses to comply with trade embargoes or face penalties

With Ukraine in turmoil, the United States government and the European Union announced the designation of a number of Ukrainian individuals, in response to the tumultuous events unfolding. By the middle of March, Russia’s duma had “welcomed” the Crimea into its fold, in effect annexing the largely Russian-speaking peninsula. Again, the West responded rapidly, targeting more individuals and, in the case of US sanctions, the businesses they own or control.

Though limited and uncertain in development, the development was a picture-perfect illustration of how, while other legislation can take years or decades to draw up, sanctions tend to be imposed with abrupt rapidity.

Sanctions and economic embargoes have been used as a tool of foreign policy for millennia, though never before has it been as complex and multifaceted as today, with companies and financial institutions needing to implement new compliance frameworks. While the sanctions tool is a powerful means of exerting political pressure, crucially, it must afford due process to those it affects directly.

“Reading the signals

Steps to comply with sanctions and limit exposure

Screen parties to transactions (e.g., customers, suppliers, distributors, transportation companies, banks) against comprehensive designated party lists

Perform due diligence with respect to ownership of parties to transactions, including beneficial ownership

Perform heightened due diligence with respect to transactions where there are red flags or otherwise may be a reason to believe a designated entity is benefiting from a transaction that on its face does not involve one

Consider additional contractual language and other protections in contracts and transaction documents to cover current or future sanctions

Review and ensure that compliance programs are robust and effective, with adequate procedures and training programs, and are updated to account for expanding sanctions

Monitor and anticipate possible future sanctions

Seek OFAC or other authorization, wherever necessary

Sanctions and export controls can hit hard and fast

It is not only the severity of the potential fines, but also the reputational impact of these actions that have convinced business to take sanctions seriously

It is not only the severity of the potential fines, but also the reputational impact of these actions that have convinced business to take sanctions seriously, and put in place sophisticated internal compliance procedures, training programs and screening mechanisms to ensure they’re not conducting business with sanctioned parties. Investigations typically arise through one of two scenarios, either for the faint-hearted. It is to be effective and convincing, it requires the utmost candour. It is time-consuming and often expensive.

Given the ever-widening scope of both international business and sanctions, which as recent events have proven can hit hard and fast, it is likely that an increasing number of businesses will either consider commissioning investigations into their own activities—or be left with little choice but to do so.

Sanctions and export controls can hit hard and fast

With Ukraine in turmoil, the United States government and the European Union announced the designation of a number of Ukrainian individuals, in response to the tumultuous events unfolding. By the middle of March, Russia’s duma had “welcomed” the Crimea into its fold, in effect annexing the largely Russian-speaking peninsula. Again, the West responded rapidly, targeting more individuals and, in the case of US sanctions, the businesses they own or control. Though limited and uncertain in development, the development was a picture-perfect illustration of how, while other legislation can take years or decades to draw up, sanctions tend to be imposed with abrupt rapidity.

Sanctions and economic embargoes have been used as a tool of foreign policy for millennia, though never before has it been as complex and multifaceted as today, with companies and financial institutions needing to implement new compliance frameworks. While the sanctions tool is a powerful means of exerting political pressure, crucially, it must afford due process to those it affects directly.

“Reading the signals

Steps to comply with sanctions and limit exposure

Screen parties to transactions (e.g., customers, suppliers, distributors, transportation companies, banks) against comprehensive designated party lists

Perform due diligence with respect to ownership of parties to transactions, including beneficial ownership

Perform heightened due diligence with respect to transactions where there are red flags or otherwise may be a reason to believe a designated entity is benefiting from a transaction that on its face does not involve one

Consider additional contractual language and other protections in contracts and transaction documents to cover current or future sanctions

Review and ensure that compliance programs are robust and effective, with adequate procedures and training programs, and are updated to account for expanding sanctions

Monitor and anticipate possible future sanctions

Seek OFAC or other authorization, wherever necessary

Sanctions and export controls can hit hard and fast

With Ukraine in turmoil, the United States government and the European Union announced the designation of a number of Ukrainian individuals, in response to the tumultuous events unfolding. By the middle of March, Russia’s duma had “welcomed” the Crimea into its fold, in effect annexing the largely Russian-speaking peninsula. Again, the West responded rapidly, targeting more individuals and, in the case of US sanctions, the businesses they own or control. Though limited and uncertain in development, the development was a picture-perfect illustration of how, while other legislation can take years or decades to draw up, sanctions tend to be imposed with abrupt rapidity.

Sanctions and economic embargoes have been used as a tool of foreign policy for millennia, though never before has it been as complex and multifaceted as today, with companies and financial institutions needing to implement new compliance frameworks. While the sanctions tool is a powerful means of exerting political pressure, crucially, it must afford due process to those it affects directly.

“Reading the signals

Steps to comply with sanctions and limit exposure

Screen parties to transactions (e.g., customers, suppliers, distributors, transportation companies, banks) against comprehensive designated party lists

Perform due diligence with respect to ownership of parties to transactions, including beneficial ownership

Perform heightened due diligence with respect to transactions where there are red flags or otherwise may be a reason to believe a designated entity is benefiting from a transaction that on its face does not involve one

Consider additional contractual language and other protections in contracts and transaction documents to cover current or future sanctions

Review and ensure that compliance programs are robust and effective, with adequate procedures and training programs, and are updated to account for expanding sanctions

Monitor and anticipate possible future sanctions

Seek OFAC or other authorization, wherever necessary
This increased regulatory and legal scrutiny has put a spotlight on previously unknown and little-understood trading practices, and demonstrates how technological advancements often outstrip investigatory and regulatory priorities and resources.

Shining a light on dark pools

Since its emergence roughly a decade ago, HFT has been largely unregulated and dominated by a few specialized and unknown proprietary trading shops. At its peak in 2009, it was estimated that HFT accounted for about 60 percent of average daily trading on US stock exchanges, bringing in an overall profit of almost US$5 billion. Although profits have declined in recent years, HFT still accounts for a significant percentage of average daily trading in US markets. ("Declining US High-Frequency Trading," New York Times, October 15, 2012.) In the wake of the increased media and public attention triggered by Lewis’s incendiary assertions regarding HFT, US regulators (and, indeed, other regulatory bodies around the world) have stepped up their scrutiny of such trading practices in an effort to allay concerns that HFT exploits ordinary investors and increases market instability. This increased regulatory focus has resulted in proposals by the SEC (and other regulators, notably in Europe) that would require high-frequency traders to, among other actions, register with regulators as broker dealers, thereby subjecting themselves to the compliance requirements and controls of these regulatory agencies.

Regulators have also now trained their sights on so-called “dark pools”—unregulated, private exchanges, often owned and operated by large investment banks, where an estimated 40 percent of US equities are now traded and which have facilitated the growth of HFT. ("SEC Chairman Targets Dark Pools, High-Speed Trading," Wall Street Journal, June 6, 2014.) As part of its call for greater transparency in the operation of dark pools, the SEC has criticized the SEC has criticized (and, in at least one instance, sanctioned) registered exchanges for practices such as “co-location”—that is, allowing HFT firms to site their computer servers alongside exchange servers to obtain a greater speed advantage. Other activities now on the US government’s radar include allowing the use of complex order types favored by high-frequency traders and orchestrating “payment for order flow” programs that incentivize brokers to divert customer trades to exchanges where high-frequency traders operate. Similarly, brokerages have been openly criticized for routing customer trades into exchanges offering the highest trading rebates, perhaps at the expense of the customer’s right to “best execution” of their trade.

In addition to the SEC, in the US other regulatory bodies including the CFTC, FINRA, Department of Justice, the FBI and the New York State Attorney General’s office, have each announced investigations into high-frequency traders and other industry participants, accusing them of profiting unfairly at the expense of ordinary investors through their use of sophisticated technology, speed advantage and utilization of complex order types.

The New York State Attorney General has been the most active so far, issuing subpoenas and letters of inquiry to exchanges and dark pool operators seeking information concerning how these trading venues have facilitated HFT. In addition, the Attorney General’s Office recently filed a complaint against a major European bank, alleging that it lied to investors by claiming its dark pool was safe from “predatory” high-frequency traders when, in fact, it had deliberately courted such traders to its exchange, concealing their presence from customers. As these investigations proceed, it becomes increasingly likely that additional exchanges, financial institutions and trading outfits will find themselves the subject of regulatory inquiry, if not legal enforcement action.

As these investigations proceed, it becomes increasingly likely that additional exchanges, financial institutions and trading outfits will find themselves the subject of regulatory inquiry, if not legal enforcement action.

Stuart Willey, Partner, White & Case, London

The European Commission has published legislative proposals, known as “MiFID II,” which introduce closer regulation and monitoring of HFT. MiFID II will impose detailed requirements on trading venues and the firms that trade on them. HFT firms engaging in proprietary trading will need to be authorized, and the rules will impose liquidity provision requirements on market making agreements between firms and venues. Trading venues will be required to set limits on the maximum number of order cancellations that a market participant can send relative to the number of transactions they undertake, and venues will be able to create fee structures for excessive order cancellation and systems use. Any firm deploying a trading algorithm will in the future be required to notify its regulator and relevant

Increased regulatory and legal scrutiny has put a spotlight on previously unknown and little-understood trading practices

Paul Catberry, Partner, White & Case, New York

Increased regulatory and legal scrutiny has put a spotlight on previously unknown and little-understood trading practices. Michael Lewis, in Flash Boys, contends that high-frequency traders, along with complicit brokers and stock exchanges, have essentially “rigged” the equities markets by using superior technology to “rigged” the equities markets (HFT), which relies on high speed data transmission technology and computer algorithms to trade quantities of complex order types favored by high-frequency traders and orchestrating “payment for order flow” programs that incentivize brokers to divert customer trades to exchanges where high-frequency traders operate. Similarly, brokerages have been openly criticized for routing customer trades into exchanges offering the highest trading rebates, perhaps at the expense of the customer’s right to “best execution” of their trade.

Increased regulatory and legal scrutiny has put a spotlight on previously unknown and little-understood trading practices. Michael Lewis, in Flash Boys, contends that high-frequency traders, along with complicit brokers and stock exchanges, have essentially “rigged” the equities markets by using superior technology to “rigged” the equities markets (HFT), which relies on high speed data transmission technology and computer algorithms to trade quantities of complex order types favored by high-frequency traders and orchestrating “payment for order flow” programs that incentivize brokers to divert customer trades to exchanges where high-frequency traders operate. Similarly, brokerages have been openly criticized for routing customer trades into exchanges offering the highest trading rebates, perhaps at the expense of the customer’s right to “best execution” of their trade.

As these investigations proceed, it becomes increasingly likely that additional exchanges, financial institutions and trading outfits will find themselves the subject of regulatory inquiry, if not legal enforcement action.

Stuart Willey, Partner, White & Case, London

The European Commission has published legislative proposals, known as “MiFID II,” which introduce closer regulation and monitoring of HFT. MiFID II will impose detailed requirements on trading venues and the firms that trade on them. HFT firms engaging in proprietary trading will need to be authorized, and the rules will impose liquidity provision requirements on market making agreements between firms and venues. Trading venues will be required to set limits on the maximum number of order cancellations that a market participant can send relative to the number of transactions they undertake, and venues will be able to create fee structures for excessive order cancellation and systems use. Any firm deploying a trading algorithm will in the future be required to notify its regulator and relevant

The European Commission has published legislative proposals, known as “MiFID II,” which introduce closer regulation and monitoring of HFT. MiFID II will impose detailed requirements on trading venues and the firms that trade on them. HFT firms engaging in proprietary trading will need to be authorized, and the rules will impose liquidity provision requirements on market making agreements between firms and venues. Trading venues will be required to set limits on the maximum number of order cancellations that a market participant can send relative to the number of transactions they undertake, and venues will be able to create fee structures for excessive order cancellation and systems use. Any firm deploying a trading algorithm will in the future be required to notify its regulator and relevant
trading venues and may be required to produce descriptions of its trading strategies and to provide assurance as to the controls the firm has instituted to ensure its algorithmic trading cannot spin out of control. The proportion of equity trading that can occur in dark pools without pre-trade transparency will also be limited by new (complex) EU-wide legislation.

While MiFID II remains a work in progress, there are differing views across Europe as to the appropriate regulatory approach. Germany has already implemented regulations covering HFT such that investment firms and other market players carrying out high-frequency algorithmic trading on the German market are now subject to supervision and must submit documentation to BaFin, the German regulator, in order to obtain authorization to conduct such trades. Authorities in Italy have introduced a tax on high-frequency equity and derivative trades. On the other hand, in the UK the Financial Conduct Authority (FCA), the UK regulator, has adopted what it describes as a risk-based approach. In a recent speech at the Global Exchange and Brokerage Conference, Martin Wheatley, CEO of the FCA, said that the FCA was adopting a three-pronged approach, namely, analysis-led policy work to get rules in shape with the bulk of the work being absorbed in gearing the UK up for MiFID II implementation; day-to-day supervision of relevant firms and markets applying a risk-based approach; and active market surveillance.

Nothing to see here

Despite increased scrutiny and the accusations leveled against HFT, some maintain that all is well within US markets. For instance, Mary Jo White, chairwoman of the SEC, recently insisted to Congress that “the markets are not rigged” and “the retail investor is … very well served by the current market structure.” These sentiments echo the assertions of defenders of HFT who claim that their practices increase market liquidity, improve price-discovery, i.e., the ability to trade stocks at fair value, and decrease trading costs due to the narrowing of buy-sell spreads. This is consistent with the SEC’s focus on enacting further reforms aimed at ensuring greater transparency and accountability in the market rather than eliminating HFT entirely.

The future

In addition to increased regulatory scrutiny, at least in the US, the private class action plaintiffs’ bar has also zeroed in on HFT by filing a number of lawsuits in federal court on behalf of investors alleging the actions of high-frequency trading firms, brokers and exchanges violated US securities laws. While the legal theories underlying these class action lawsuits appear somewhat suspect—for instance, it is not clear how a high-frequency trader’s use of faster trading technology to beat another investor’s order to market violates US law—we anticipate that such theories will evolve and develop as regulators uncover (and publicize) additional information concerning how HFT firms and dark pools operate.

“I have little doubt that the plaintiffs’ bar is intently focused on the various regulatory investigations currently under way in the US and elsewhere with the objective of further developing their understanding of these trading practices so they can craft the next wave of claims against various market participants. The complaint recently filed against a dark pool operator by one of its customers piggybacking off of the charges asserted by the New York Attorney General against the same bank, only goes to show that this is a strategy likely to be pursued by other plaintiffs’ lawyers in the future,” said US securities litigator and White & Case partner Greg Little. Despite the specter of heightened regulation, further legal enforcement action and private lawsuits, HFT is likely to remain a significant feature of equities markets globally with ever-increasing influence in equity markets across Europe, Asia and Latin America. Over time, HFT is also likely to infiltrate further into non-equities markets as well. Ongoing advances in computer and data transmission technologies, such as transmitting orders by microwave, continue to promise traders the ability to profit from trades executed on the basis of increasingly small increments of a second. It is, therefore, inevitable that governmental regulators, as well as those in the media and the public at large, will demand exacting oversight and scrutiny of the new technologies and the trading practices spawned by them.

Reading the signals

HFT—future regulatory scrutiny

- Monitor activity of the US private class action plaintiffs’ bar
- Follow EU-wide MiFID II developments
- Be aware of differing regulatory regimes across Europe
- Be alert to the infiltration of HFT practices into non-equities markets

The Plaintiff’s bar is intently focused on the various regulatory investigations currently under way so they can craft the next wave of claims against various market participants

Greg Little, Partner, White & Case, New York