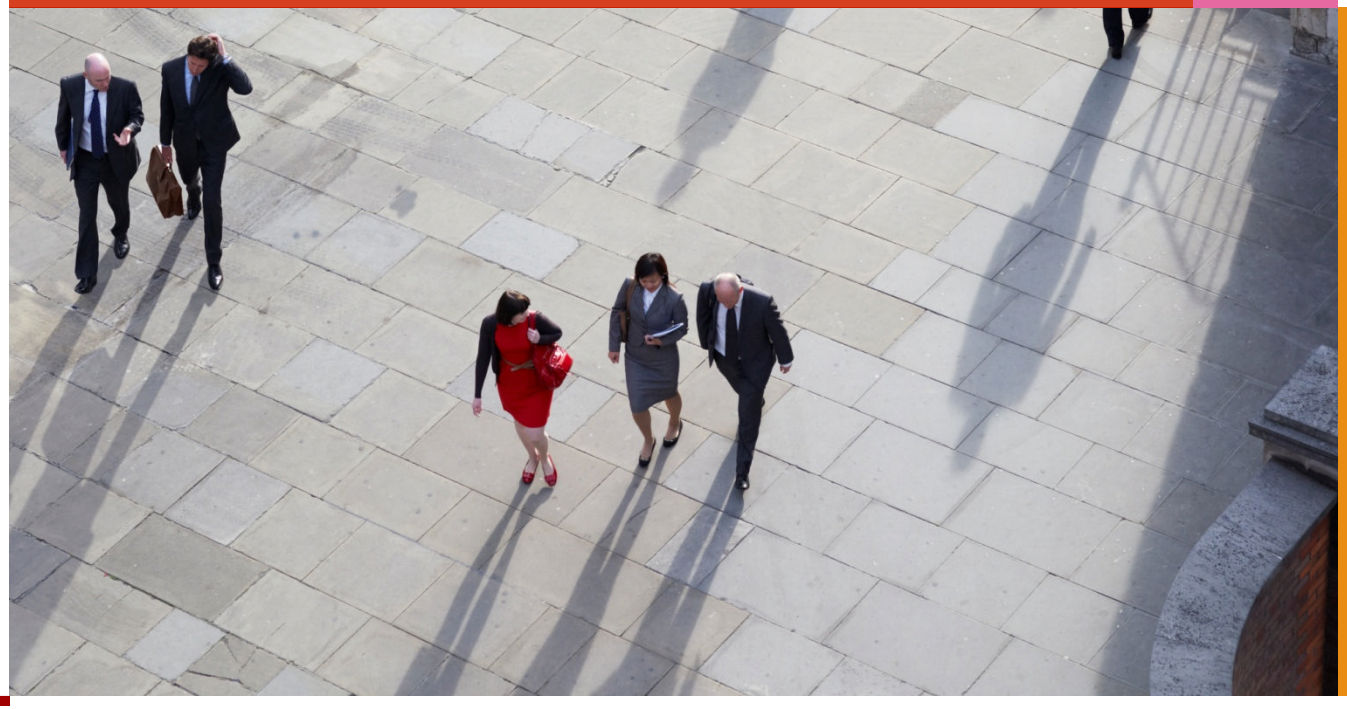
A publication of PwC's Financial Services Institute (FSI)

Avoiding the Headlines: How Financial Services Firms Can Implement Programs to Prevent Insider Trading



pwc

Contents

Section		Page
1.	Point of view	2
2.	A deeper dive into insider trading	14
3.	Current situation	20
4.	A framework for response	30
5.	How PwC can help	40
Appendix	Select qualifications	46

Section 1

Point of view

Point of view

Financial services firms of all types face serious risks if they lack effective programs to prevent and detect illegal insider trading.

Illegal insider trading can impact all types of firms, and can put the franchise at risk.

Recent civil and criminal investigations have implicated all types of firms, including hedge funds, mutual funds and other types of asset management firms, banks, broker-dealers, public companies, law firms, and accounting firms.

For traders and tippers, the consequences of insider trading can be serious and can include jail time, financial penalties, and being barred from the industry.

For financial services firms, the consequences of an employee, officer, or director being accused of insider trading can be highly damaging—and can destroy client, investor, and public trust in the firm. Even a rumor about an insider trading investigation can result in damaging asset flight and a cloud over a firm's ability to do business. If your firm lacks a robust program to prevent and detect insider trading, it is at risk—as the actions of a single employee can be devastating for the firm.

In PwC's view, senior managers, boards of directors, general counsels, chief compliance officers, and internal auditors should be taking a hard look at their existing programs and controls to make sure that they are meeting today's regulatory expectations and using the most current arsenal of tools to protect their firms from insider trading and its damaging consequences.

Financial services firms have a legal obligation to establish programs to prevent and detect insider trading.

While it is good business, the law also requires, and regulators expect, that firms will have robust compliance, supervisory, surveillance, and control measures in place. Regulators can bring enforcement action for the failure to have an adequate insider trading prevention program—even if no insider trading has occurred.

Point of view

Insider trading has become a top priority of prosecutors. And civil and criminal regulators are working closely together, both in the United States and abroad.

Detecting and prosecuting insider trading is a high priority for criminal and civil prosecutors today.

The Securities and Exchange Commission (SEC) and the Department of Justice (DOJ) have stepped up surveillance, investigations, and prosecutions. Preet Bhahara, the US Attorney for the Southern District of New York, said that "insider trading is rampant" and "the investigation and prosecution of illegal insider trading has been, and will remain, a top criminal priority" ("*The Future of White Collar Enforcement: A Prosecutor's View,*" Before the New York City Bar Association, October 20, 2010).

Criminal investigators and prosecutors are using tools once reserved for organized crime and narcotics investigations to detect and investigate insider trading—wiretaps, cooperation agreements, bounties, and search warrants—as well as sophisticated data analysis. Recent cases and investigations show increased cooperation among civil and criminal regulators, both in the United States and abroad.

Illegal insider trading harms the public trust in the fairness of the securities markets and undermines the system of fair disclosure of material information to the markets. Indeed, following the recent insider trading cases, individual investors were quoted as saying that the cases confirmed their suspicion that the markets were "rigged."

When regulators detect insider trading, they are seeking to generate attention for cases and to increase sanctions—to increase the deterrent impact of their cases.

Seeking appropriate sanctions commensurate with wrongdoing is not the regulators' only goal. Especially in cases that involve insider trading "rings" with serial insider trading activity, regulators are likely to seek sanctions that will have a strong deterrent effect on others. As a result, cases are likely to result in stiff fines set at multiples of the profit obtained and, in some cases, jail time. Press conferences and "perp walks" are also part of the strategy.

Point of view

Sanctions for insider trading can be serious. Beyond disgorgement of profits obtained or losses avoided—and being suspended or barred from the industry—criminal sanctions include hefty financial penalties and jail time.

Insider trading is expensive for both companies and individuals.

- Cases often result in "disgorgement" of any money made or losses avoided, as well as penalties of up to three times the amount disgorged.
- A person who "tips" another but does not trade may also be required to pay disgorgement and penalties of anyone he/she tipped.
- A trader/tipper who is associated with the securities industry may be suspended or barred from the industry.
- Criminal sanctions include financial penalties and jail time.
- For firms, if insider trading occurs and the firm failed to prevent or detect it reasonably, the firm may also be required to pay penalties, and may be suspended or barred from the industry.
- If a firm lacks an adequate program to prevent and detect insider trading, it may be subject to enforcement action by the SEC—even if no insider trading occurs.

Beyond the sanctions that may be imposed, insider trading damages reputations and careers. In our view, prevention is truly worth the cost.

Point of view

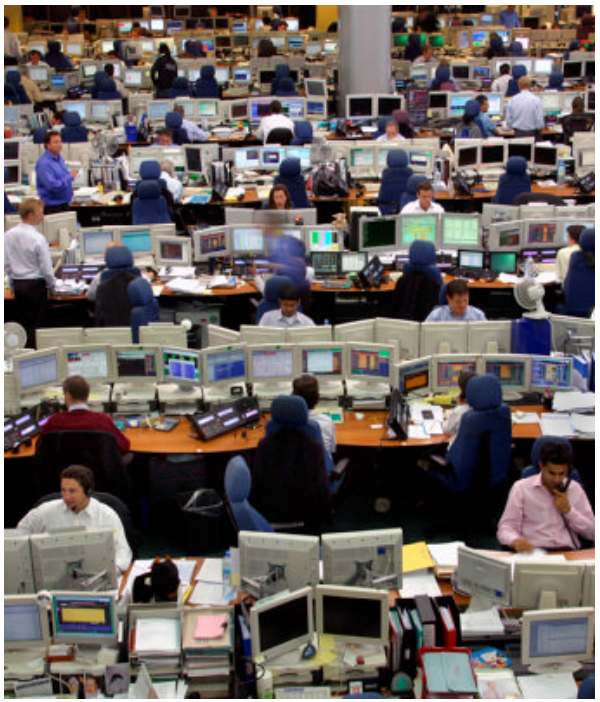
Not all insider trading is illegal. Knowing the distinction is critical.

What is insider trading? What makes some insider trading illegal?

Generally speaking, insider trading is trading in a company's stock by an "insider"—for example, a company employee, officer, director, or other person. When these individuals purchase or sell company stock without taking advantage of nonpublic information, it is lawful (for example, as part of employee benefit plans or pursuant to a preexisting plan to purchase/sell the stock).

Illegal insider trading occurs when a person buys or sells a security when in possession of material nonpublic information in violation of a duty of trust or confidence that the person owes to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information.

Even for people who are not classic "insiders," it is a violation of the law to "misappropriate" material nonpublic information and to trade on it or to pass the information on to another in violation of a duty of confidentiality.

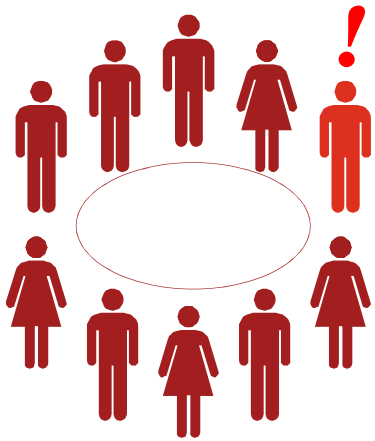


Point of view

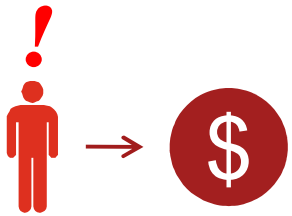
Examples of illegal insider trading.

For example, it would be illegal for a corporate insider (such as an employee, officer, or director) or a "temporary" insider (such as a person who is providing services to a company such as a lawyer, accountant, or a vendor) to trade securities while in possession of material nonpublic information about the issuer of such securities.

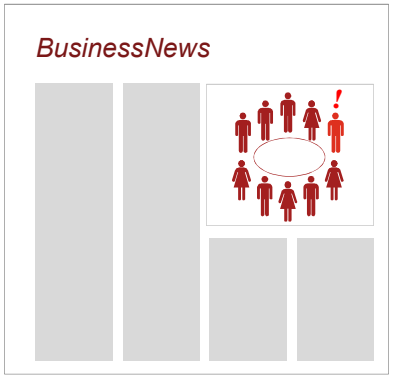
It is also illegal to provide (or "tip") another person with the information, and for that person to trade on it or tip another, if he/she knows, or should know, that the insider has given him/her nonpublic information in breach of a duty.



One bad actor in the boardroom...



Takes inside information out to trade...



...Before the information is made public.

Point of view

Current investigations and cases involve the use of "expert networks"—more actions are yet to come.

On November 20, 2010, *The Wall Street Journal* (WSJ) reported that the SEC and the DOJ were investigating insider trading by hedge funds and other asset management firms.

According to the WSJ's report and follow-up coverage, the probe focuses on the use of "expert-network" research consultants who provide asset managers with insights into various industries, including but not limited to technology, healthcare, and retail.

What are "expert networks"?

"Expert networks" are consulting firms that connect experts on a host of topics with traders, analysts, and others seeking information on these topics. Occasionally, such "experts" may hold or have held positions with, or have contacts with, some of the issuers about which they provide information. In some cases, experts have been physicians who are involved in clinical trials of new drugs and treatment regimens. Others provide "channel checking" information about, for example, retail sales or consumer traffic at a particular location. Expert networks charge fees to clients in return for access to the experts.

What is the status of the insider trading investigation into "expert networks"?

Investigations are active and ongoing. Thus far, more than a dozen individuals have been charged. Charges have been brought against the experts alleged to have provided material nonpublic information (MNPI) as well as against the hedge fund managers accused of insider trading. A number of individuals are cooperating with prosecutors as the investigations continue.

Point of view
What are the risks of using experts?

Are "expert networks" illegal?

No, but contact with certain kinds of experts may raise suspicion that the expert functions as a conduit for material nonpublic information about particular issues. Given the risks, controls are imperative.

How are organizations that use expert networks managing the related risks?

Firms that use experts are establishing controls and surveillance to address these risks. These compliance and control mechanisms are intended to:

1) Indicate the firm's intent that it does not want to receive MNPI from an expert.
2) Document and supervise the use of expert consultants and resulting trading.
3) Surveil and review the use of expert consultants and trading.
4) Inform and train firm employees on the risks and the firm's policies to prevent receiving/trading on MNPI.

For example, it is becoming increasingly common for those who use expert networks to revise their contracts with such consultants to explicitly state that the manager does not want to receive confidential or material nonpublic information (MNPI). It is also becoming increasingly common to require the expert consultant to warrant that the consultant will not provide confidential information or MNPI.

Leading firms are putting effective controls in place and taking a myriad of steps to mitigate the risks of trading while in possession of MNPI.

Point of view

While most insider trading cases have involved equity securities, insider trading prohibitions extend to other types of securities as well.

Credit default swaps	The SEC alleged that a portfolio manager at a hedge fund investment adviser and a bond salesman engaged in insider trading in credit default swaps (CDS). The bond salesman allegedly tipped the portfolio manager that a proposed change to a bond offering was expected to increase the price of the CDS on the bonds, and the portfolio manager then purchased the CDS. The court appeared to accept the SEC's view that traders in CDS could be liable under insider trading prohibitions. (SEC v. Rorech)
Mutual fund shares	The SEC alleged that a mutual fund management company executive learned that the fund might soon reduce the value it assigned to several of its mortgage-backed securities holdings—a move that would likely decrease the fund's per-share net asset value (NAV). The executive redeemed all of his fund shares and caused a family member to do the same. He was subsequently charged with insider trading in the mutual fund's shares. (SEC v. Marquardt and SEC v. Baldt)
Treasury bonds	The SEC alleged that, after learning that the Treasury Department was suspending future long bond issuances, and despite having agreed to keep the information embargoed, an individual notified a portfolio manager at a mutual fund complex of the news. Before the news became public, the portfolio manager and other portfolio managers allegedly bought $65 million in par value of 30-year bonds for funds that they managed, generating approximately $3.1 million in illegal profits. (SEC v. Nothern)
Auction rate securities	A financial services executive who allegedly had nonpublic information about the impending failure of the auction rate securities market sold his entire holdings before the auctions occurred. The executive was charged with insider trading and settled the case for $2.75 million. (NY v. Shulman)
Options	A private equity firm employee allegedly tipped friends using coded messages as to his firm's negotiations with certain public companies. The friends traded options issued by the public companies and kicked back some proceeds to the tipper. (SEC v. Gowrish)

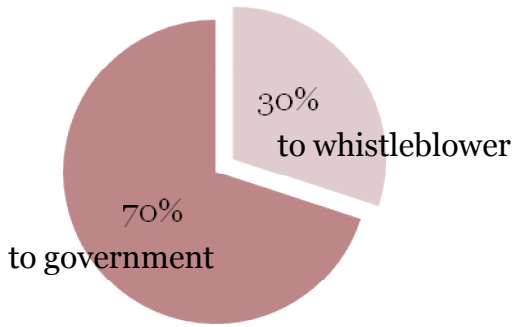
Point of view

Scrutiny will only increase—the SEC's new whistleblower program will result in pressure on firms' compliance programs.

While the SEC has long had authority to pay bounties to "whistleblowers" in insider trading cases, it has seldom used its authority. According to an SEC Inspector General Report, the SEC has paid only $159,537 to five whistleblower claimants since 1989. On July 23, 2010, however, the SEC announced that it had paid a bounty of $1 million dollars to a whistleblower in an insider trading case. (SEC v. Pequot)

The Dodd-Frank Act will incent whistleblowers

Up to 30% of any amounts recovered can be used to reward whistleblowers.



The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) provides the SEC with authority to create a new whistleblower program, and to pay bounties of between 10% and 30% of any amounts recovered based on the whistleblower's information.

This new authority, and the publicity that has surrounded it, is likely to inspire many more complaints and tips to the SEC about all manner of alleged violations.

Because it is very difficult, if not impossible, to assess the veracity of complaints and tips from the face of the information, the SEC will likely initiate additional examinations and investigations to follow up on these new allegations.

When complaints or tips allege insider trading, a key part of the SEC's inquiry will be whether the registered securities firm has an adequate program in place to prevent and detect insider trading.

As a result, we think that the adequacy of securities firms' programs to prevent and detect insider trading will face new scrutiny.

Point of view

With insider trading a top priority, leading firms are reviewing their existing protocols to prevent insider trading and are making changes.

We have observed leading financial institutions making the following types of changes:

- Conducting current assessments of the possible sources of MNPI across the firm.
- Reviewing and enhancing firewalls.
- Implementing new controls over the use of experts and any trades in names where an expert was used.
- Identifying high-risk areas and activities based on the firm's activities and personnel and conducting special reviews of controls and trading.
- Implementing new control and surveillance tools.
- Conducting new and tailored employee education.

Point of view

Financial services firms must have programs to prevent and detect insider trading—it's the law.

The law requires firms to act.

- ***Registered investment advisers must*** "establish, maintain, and enforce written policies and procedures reasonably designed … to prevent the misuse … of material, nonpublic information by such investment adviser or any person associated with such investment adviser." (Section 204A of the Investment Advisers Act of 1940)
- ***Registered broker-dealers must*** "establish, maintain, and enforce written policies and procedures reasonably designed … to prevent the misuse … of material, nonpublic information by such broker or dealer or any person associated with such broker or dealer." (Section 15(f) of the Securities Exchange Act of 1934)

The obligation to prevent and detect insider trading is serious—and firms and supervisors can be sued for having faulty programs, even if no insider trading has occurred.

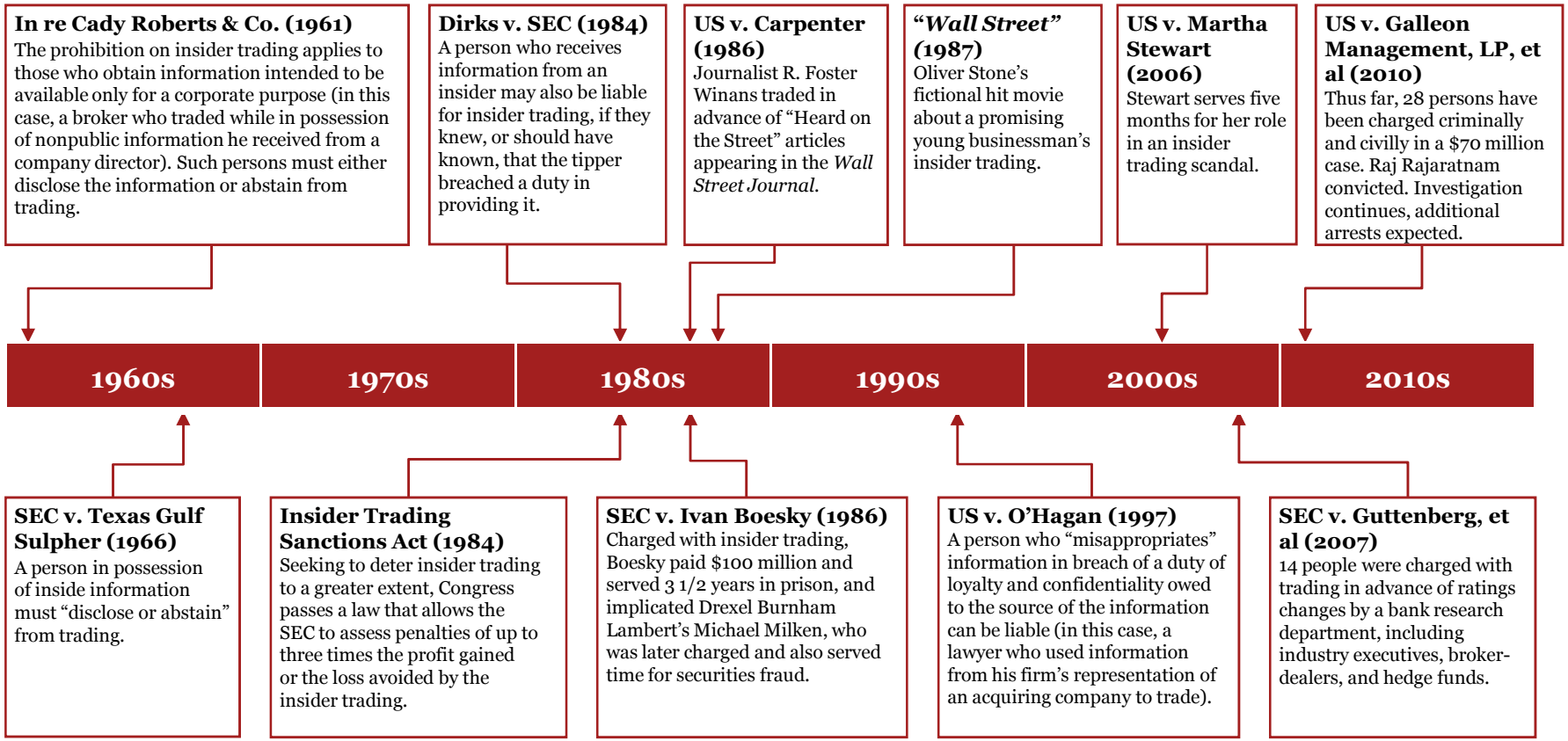
- Even though no instance of insider trading was alleged, in November 2010, a chief compliance officer (CCO) and two advisory firms were charged with failing to have adequate policies and procedures in place to prevent the misuse of nonpublic information, resulting in fines, censures, and cease-and-desist orders. (In the Matter of Buckingham Research Corp., et al.)
- In February 2009, a broker-dealer firm supervisor was charged with failing reasonably to supervise a managing director who engaged in insider trading—allegedly by selling shares short in his own account while in possession of MNPI obtained through a solicitation to participate in a private investment in public equity (PIPE) transaction. The supervisor was charged with failing to follow up on red flags indicating that the managing director's trading was questionable. The supervisor paid a fine, and the firm paid more than $8 million in disgorgement and interest. (In the Matter of SG Americas Securities, LLC, et al.)

Section 2

A deeper dive into insider trading

A deeper dive

Insider trading: select milestone events



Source: http://www.sec.gov/litigation/litreleases.shtml

A deeper dive

What is "material" information?

Information is *material* if there is a substantial likelihood that a reasonable investor would consider it important in making an investment or trading decision. It does not have to be the most important information; it can be one of many factors.

Examples of information predicating insider trading cases:

Organizational changes	Financial information	Operational developments	Securities information
• Mergers, acquisitions, or similar transactions • Significant personnel changes • Change in control • Receiverships	• Earnings • Sales figures • Accounting restatements • Change in auditors or auditor notification that the issuer may no longer rely on an auditor's report • Bankruptcies	• New product plans • Developments regarding customers • Major supplier changes (such as the acquisition or loss of a contract) • FDA or other government approvals	• Defaults on senior securities • Calls of securities for redemption • Repurchase plans • Stock splits • Changes in dividends • Changes to the rights of security holders • Public or private sales of additional securities

Material nonpublic information about or concerning a public company does not need to derive from the company itself, for example:

- Advance notice of large pending or planned orders to buy/sell the company's stock
- A planned acquisition of the company
- An analyst's ratings upgrade or downgrade
- A financial columnist's view of the company

A deeper dive

Information must be "material" and "nonpublic," but a trader need not *rely* on the information when trading to be found liable.

What is "nonpublic" information?

Nonpublic information is knowledge of an event, plan, or information (financial, competitive, or otherwise), which has not been disseminated to the public via media, financial publications, Bloomberg, Reuters, prospectuses, proxy statements, company press releases, or other means. Information received "in confidence" is likely nonpublic, including information received pursuant to a nondisclosure or confidentiality agreement.

Must the trader have actually relied on the information in question?

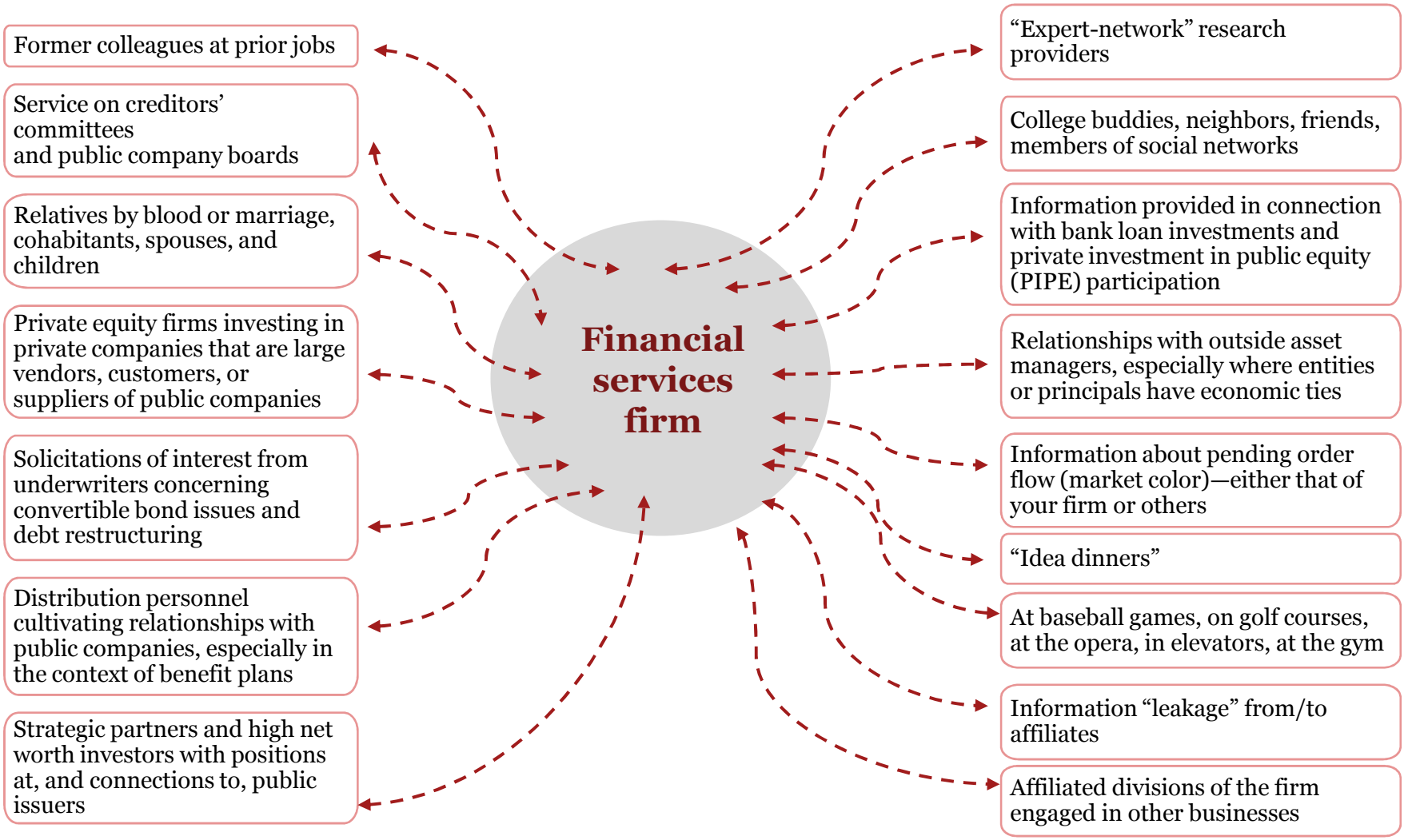
According to the SEC, it is not necessary to show that the trader actually used or relied on the information when trading, but only that the trader traded *while in possession* of such information. The information need not have affected the trader's opinion, so long as it was material; it was nonpublic; and he/she knew, or should have known, that it was obtained in violation of a duty of trust or confidence.

Consequences of receiving MNPI.

This means that receiving MNPI will immediately prohibit further trading in the stock—even when the MNPI would not in itself have led to a decision to trade. For example, a portfolio manager or trader may be conducting an extensive original analysis on a stock. If he receives MNPI, he cannot trade the stock—even if he made the decision to trade *before* receiving the MNPI, or he had *already started* to undertake the trade when he received MNPI, or the MNPI was *irrelevant* to his decision to trade. The prohibition on trading while in possession of MNPI effectively shuts down the possibility of using the original analysis until after the MNPI has become public. The prohibition on trading could expose a firm with a short position to significant losses.

A deeper dive

Material nonpublic information can come from a large variety of sources.



A deeper dive

"Tipping" can subject a person to the same consequences—just as if he/she traded on nonpublic information.

What is a "tipper"?

A tipper is a person who provides MNPI to another in violation of a duty of trust or confidence.

What is a "tippee"?

A tippee is a person who receives information from a tipper—information that the tippee knows, or reasonably ought to know, is being provided in violation of a duty of trust or confidence, and then trades or tips another.

Both "tippers' and "tippees" can be liable.

A tipper may be liable for the insider trading of a "tippee," even when the tipper did not himself trade.

Like persons who trade while in possession of MNPI, tippers may be liable for penalties up to three times the profit earned from, or loss avoided by, the actual trader. Other civil and criminal penalties may apply as well.

It starts off as a friendly game of golf, but your chatter matters.

When does a "duty of trust or confidence" exist?

A duty of trust or confidence exists in the following circumstances, among others:

- Whenever a person agrees to maintain information in confidence.
- Whenever the person communicating the material nonpublic information and the person to whom it is communicated have a history, pattern, or practice of sharing confidences, such that the recipient of the information knows, or reasonably should know, that the person communicating the material nonpublic information expects that the recipient will maintain its confidentiality.
- Whenever a person receives or obtains material nonpublic information from his or her spouse, parent, child, or sibling. (Exchange Act Rule 10b5-2)

Section 3

Current situation

Current situation
Some believe that illegal insider trading has increased in recent years.

Has insider trading increased?

The US Attorney for the Southern District of New York recently said:

> *"Unfortunately, from what I can see from my vantage point as the US Attorney here, illegal insider trading is rampant and may even be on the rise. And the people who are cheating the system include bad actors not only at Wall Street firms, but also at Main Street companies. Disturbingly, many of the people who are going to such lengths to obtain inside information for a trading advantage are already among the most advantaged, privileged, and wealthy insiders in modern finance. But for them, material nonpublic information is akin to a performance-enhancing drug that provides the illegal "edge" to outpace their rivals and make even more money. In some respects, inside information is a form of financial steroid. It is unfair; it is offensive; it is unlawful; and it puts a black mark on the entire enterprise."*

Preet Bharara, "*The Future of White Collar Enforcement: A Prosecutor's View,*" prepared remarks before the New York City Bar Association (Oct. 20, 2010)

Similarly, Robert Khuzami, the SEC's Director of Enforcement, recently noted that spikes in trading continue to precede significant announcements of M&A activity or accounting restatements, and are indicative of insider trading. (Eamon Javers, "SEC Also Conducting Insider Trading Inquiries: Khuzami," www.cnbc.com (Dec. 17, 2010))

While it is impossible to know with certainty whether illegal insider trading has increased, it may be that today's generation of traders and market participants is simply not aware of the ramifications of insider trading and is not familiar with—or deterred by—the notorious insider trading scandals and prosecutions of the 1980s. Indeed, at a recent PwC conference, former SEC Chairman Harvey Pitt stated: "We're dealing with a segment of the financial services industry that hasn't really been regulated before. It doesn't have the long experience of having compliance and infrastructure as well as being populated by people who are painfully young compared to at least some of us and who may not remember the lessons of the eighties." (PwC Alternatives Investment Seminar, Dec. 2, 2010).

Current situation

Today's cases have expanded to target organized insider trading "rings." This brand of insider trading is likely to elicit the strongest possible prosecution and penalties.

Most insider trading cases tell stories of the opportunistic insider trader—the person who happens to acquire inside information and, succumbing to temptation and greed, trades once. Today's cases, however, reflect a more organized, pervasive type of insider trading:

***SEC v. Galleon*:**

Twenty-eight people have been charged to date as part of an "insider trading ring" involving hedge fund manager Raj Rajaratnam, alleging that "a network of corporate insiders and financial professionals" including public company executives, hedge fund adviser principals and analysts, an investor relations consultant, and others made illegal profits of $70 million.

***SEC v. Arthur Cutillo, et al*:**

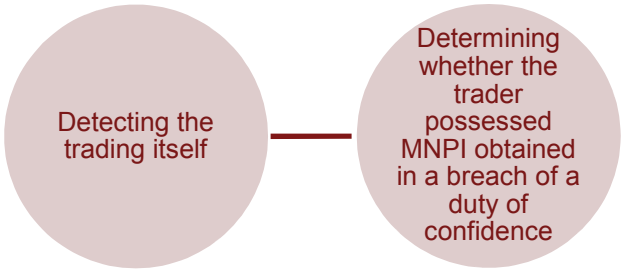
Nine people were charged in an alleged "insider trading ring" that included lawyers, professional traders, and hedge fund managers in a $20 million scheme fueled by a lawyer who divulged confidential information involving some of his firm's clients in exchange for kickbacks. One Wall Street trader was referred to as "Octopussy"—as in the James Bond movie—because of his reputation for having arms in so many sources of inside information.

SEC Director of Enforcement Robert Khuzami has said these cases may reflect a "systemic" behavior that has spread within the industry: "You have funds whose business model consisted of vigorous attempts to collect information from corporate insiders and to utilize that information to trade." Such an approach is "potentially more dangerous" than previous insider-trading cases that reflected "opportunistic" behavior. (Peter Cook, "SEC's Rob Khuzami Talks Finance Illegalities at Bloomberg Summit," *Bloomberg News*, Nov. 12, 2009).

Current situation

Regulators are combating insider trading in new ways.

There are two basic components to investigations of insider trading:



Historically, the typical means used to detect insider trading was market surveillance which revealed aberrational trades. For example, investigators would focus on a specific time period just before a public announcement and identify large, cannily-timed, or otherwise suspicious trades. Then, investigators would probe the traders to determine why they traded and their possible access to MNPI.

Regulators have improved market surveillance to detect insider trading. Investigators are now using new strategies to surveil traders themselves for the transmission of MNPI *before the trades occur*.

Investigators are no longer waiting for the trading to occur and then to be picked up in routine market surveillance. Nor do they need a confession. Most insider trading cases are brought by prosecutors who are ready to make circumstantial inferences based on the timing of trades and the trader's access to information, as well as telephone, e-mail, or other records.

Current situation

Investigators are using new detection tools, including conducting coordinated market surveillance, and are taking proactive dives into data and connections.

In both the equities and the options markets, surveillance for insider trading is now coordinated across trading markets.

Options: The Options Regulatory Surveillance Authority (ORSA), created in 2006, surveils options trading for insider trading, conducts investigations, and refers possible incidents to the SEC for investigation. According to the Chicago Board Options Exchange (CBOE), which runs ORSA, "it is responsible for detecting trading in advance of the release of nonpublic corporate information as well as research reports, analyst recommendations, and market rumors by corporate officers, directors or employees of a publicly traded company or public investors."

Equities: As of 2010, the Financial Industry Regulatory Authority (FINRA) is now responsible for insider trading surveillance of all exchange-listed and over-the-counter (OTC) equity securities across the United States, regardless of the platform on which a trade is executed. FINRA's Insider Trading Surveillance unit surveils for insider trading, conducts investigations, and refers possible incidents to the SEC for investigation (referring 244 matters to the SEC in 2010). According to FINRA, the combination of NYSE regulation and its own aggregated trade history and case repositories has created a centralized library of regulatory data that serves as an investigative tool in uncovering serial insider trading rings.

Current situation

The SEC is using new approaches to detect insider trading.

The SEC created a dedicated "Market Abuse" Unit to detect insider trading and other trading abuses.

Staffed with experienced investigators and attorneys and new market specialists to assist investigators, the Market Abuse Unit is headed by Dan Hawke, Regional Director of the SEC's Philadelphia office. According to Hawke, the unit's goal is to:

> *"Focus on suspected large-scale insider trading networks and rings—so-called "organized" insider-trading… A core objective of our unit will be to go on offense. We plan to be pro-active by identifying patterns, connections and relationships among traders and institutions at the outset of investigations… That is why a key objective will be developing and deploying automated trading data analysis. Through more sophisticated technology, we can give ourselves strategic advantages in the way we conduct complex trading investigations, particularly those involving large institutions."* (Dan Hawke, *"Remarks at News Conference Announcing New SEC Leaders in Enforcement Division,"* Washington, D.C. January 13, 2010)

The unit sifts through hundreds of millions of electronic trading records to identify groups of traders who repeatedly made similar well-timed bets.

A significant part of this new approach is to mine previously submitted reports of trading, along with conducting other detective work. A February 2010 article about the unit stated that "the team cross-checks trading data on dozens of stocks with personal information about individual traders, such as where they went to business school or where they used to work." Hawke said his investigators are looking for patterns of "behavior by traders across multiple securities" and any "common relationships or associations between those traders." (Matthew Goldstein, "*Philadelphia, Where Rogue Traders Dare Not Tread*," www.reuters.com, Feb. 19, 2010)

The Market Abuse Unit is credited with filing the insider trading enforcement case SEC v. Galleon. Twenty-eight people have been charged to date as part of an "insider trading ring" involving hedge fund manager Raj Rajaratnam, alleging that "a network of corporate insiders and financial professionals" made illegal profits of $70 million. (US Securities and Exchange Commission, Litigation Release No. 21827, Jan. 26, 2011)

Current situation

The SEC is using new approaches to detect insider trading (continued).

Comparing trading data and emails at unaffiliated firms with close associations or economic ties.

To a greater extent, the SEC is making connections among firms and conducting examinations and investigations based on those connections. A firm implicated in an insider trading investigation may find that other firms with which it has or had connections is also under scrutiny. Investigators may look for a pattern of coordinated trading (portfolio or personal) between ostensibly unaffiliated firms that have close economic ties or personal relationships among principals or portfolio managers. Investigators may also look to see whether one firm is trading securities that appear on other firms' restricted lists.

The SEC and the DOJ are performing coordinated investigations.

Civil and criminal regulators are working closely together. Insider trading is a key priority for both. To the extent permitted by grand jury secrecy rules, the agencies are sharing information. As a result, many of the largest insider trading cases in the past year have resulted in the simultaneous announcement of an SEC civil action alongside a DOJ prosecution.

Current situation

The SEC is using new approaches to detect insider trading (continued).

We are seeing more cooperation agreements between the SEC and foreign counterparts.

The SEC has increased its cooperation with foreign securities regulators, including the sharing of information with organizations such as the UK's Financial Services Authority (FSA) and Hong Kong's Securities and Futures Commission. Within the past few years, the SEC has increased the number of jurisdictions with which it has explicit agreements for information sharing. Coordinated insider trading investigations are also more common. For example, the SEC and the FSA recently brought simultaneous charges against a group of insider traders in California and in the UK, where the California residents allegedly tipped the UK residents, who then traded.

Cooperation and non-prosecution agreements between the SEC and witnesses are more common.

To obtain information, the SEC now enters into cooperation and "non-prosecution" agreements, modeled after criminal prosecutors. This initiative was announced in January 2010. At the end of 2010, the SEC announced its first such settled case in which the corporate entity involved avoided being charged by entering into a cooperation agreement and helping the staff bring its case against the individuals involved. The SEC's Deputy Director of Enforcement recently said that the SEC had entered into 20 cooperation agreements since the program was announced in January 2010. (Randall Fons, Tiffany Rowe, Morrison & Foerster, "*The SEC Speaks: Aggressive Enforcement to Intensify in 2011,*" www.mofo.com, Feb. 9, 2011)

Current situation

To detect and investigate insider trading, criminal investigators and prosecutors are using tools once reserved for organized crime and narcotics investigations.

Reflecting a new more aggressive approach, criminal investigators are using wiretaps, mass subpoenas, search warrants, and cooperation agreements in insider trading investigations—many of which are investigative tools that are unprecedented in this type of investigation.

Their use signals a more aggressive approach to insider trading and other types of financial fraud. In particular, the use of wiretaps and wires worn by cooperating witnesses has sent shock waves through the financial world, and has caused many to wonder, only half in jest, who might be on tape? Why wiretaps?

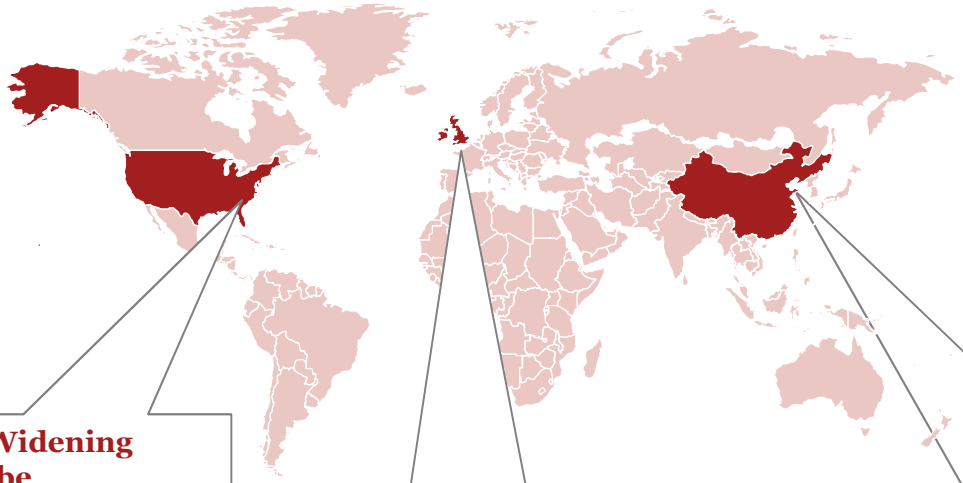
> *"It does not take a rocket scientist to understand that it would be helpful to have the actual recording of the communication." ... "I am here to tell you that court-authorized wiretaps, so long as all the legal requirements can be met, will continue to be in our toolbox in insider trading cases... And especially when sophisticated business people begin to adopt the methods of common criminals, such as the use of anonymous cell phones, we have no choice but to treat them as such. To use tough tactics in these circumstances is not being heavy handed; it is being even-handed. It would be difficult to explain to the public why alleged financial fraudsters deserve a milder approach just because they wear a white collar."*
>
> Preet Bharara, *"The Future of White Collar Enforcement: A Prosecutor's View"* (Oct. 20, 2010)

At a recent PwC/Georgetown University conference on financial reform, Denis McInerney, Chief of the Fraud Section in the US Department of Justice, spoke to just how new these tactics are:

> *"It really is a sea change from how things were... We very rarely went up on wiretaps in the securities unit (in the SDNY). We didn't do a lot of search warrants; you didn't do a lot of consensual recordings... Nowadays in the white collar world, wiretaps, consensual recordings, search warrants, they are commonplace. We're no longer treating white-collar crime in any different way from how you treat organized crime or narcotics."*
>
> (Oct. 25, 2010)

Current situation

Globally, regulators have grown more aggressive.



US Arrests 4 in Widening Hedge Fund Probe

Dunstan Prial | Dec. 16, 2010

Agents of the Federal Bureau of Investigation on Thursday morning arrested four suspects on insider-trading charges in the latest move in a US crackdown on Wall Street hedge funds and so-called expert networks.

Expert-Networking Worker Arrested for Insider Trading

CNBC.com and Wires | Nov. 24, 2010

US prosecutors arrested an employee of an "expert networking firm" on charges that he promoted the firm's services by arranging for corporate executives to leak inside information to hedge funds.

FSA Using New Tools to Pursue Insider Trading Probe

Bloomberg Business Week, March 25, 2010

FSA Fines Ex-Hedge Fund Manager for Insider Trading

Reuters, London, June 23, 2010

A former hedge fund manager was fined 50,000 pounds for insider trading.

Hong Kong Jails 2 for Insider Trading

The New York Times, July 22, 2009

A Hong Kong court on Monday jailed a former banker from a regional brokerage and an ex-fund manager for insider trading offenses, the latest action under the city's crackdown on market misconduct.

To the Dungeon: Regulators Are Suddenly Getting Tough

The Economist, Hong Kong, Sept. 17, 2009

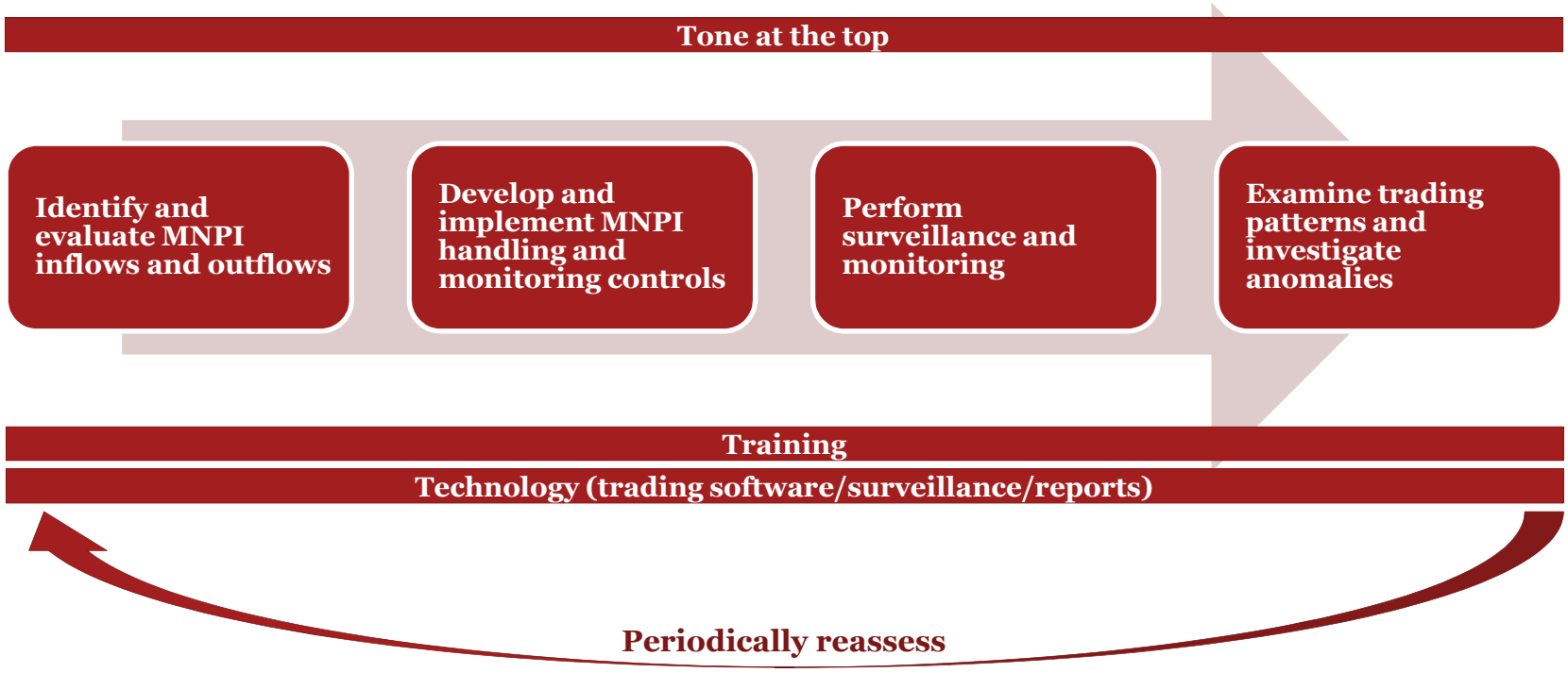
It has long been considered a paradise for investors who have a juicy bit of inside knowledge. Insider trading was not even a criminal offence in Hong Kong until 2003.

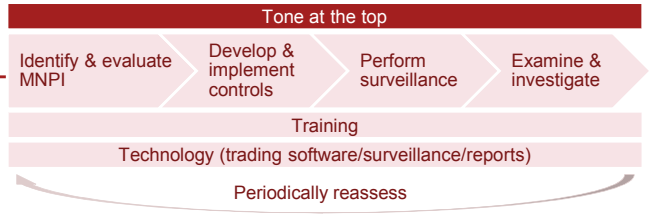
Section 4

A framework for response

A framework for response

An effective anti-insider trading program must have multiple complementary components; continually reassess risks; and be supported by consistent, clear messaging from the top.





A framework for response

Set the right tone at the top by establishing and communicating clear expectations throughout the organization.

Developing the right approach requires focusing on demonstrable and documented steps by senior management to convey a "zero tolerance" message concerning insider trading.

Key considerations:

Board oversight and tone

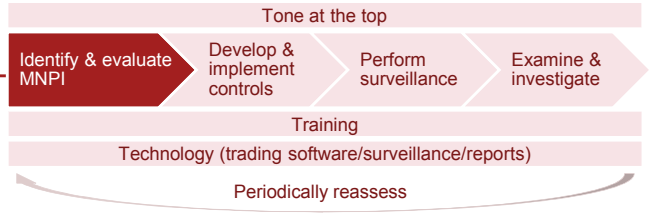
- Protect the firm.
- Make no apologies for insider trading. Convey a clear message that the firm is actively seeking to detect insider trading and will turn violators over to authorities.
- Having a formal policy in place is not enough. The policy must be robust and enforceable. Penalties for noncompliance must be communicated and enforced. Consider requiring employees to complete an annual certification of compliance with insider trading policies.

CEO and senior management

- Senior management is knowledgeable and conversant in the steps the firm is taking to combat insider trading.
- Senior management authorizes the deployment of appropriate personnel, IT, and other resources.
- Senior management endorses board-level and executive-level restrictions. For example, some insider trading policies prohibit executives from pledging, hedging, short sales, and similar activities (including through the use of derivatives).
- Senior management delivers, or at least participates, in insider trading training.

Formal policy

- Policy establishes restrictions, requirements, and responsibilities for employees based on role, level, etc. For example, executives may trade only after being given pre-clearance to trade, and blackout or holding periods may apply.
- Policy includes company-specific examples as to what could be deemed "material," both positive and negative. Policy includes guidance related to "gray areas;" communicating with relatives and friends; and information shared with third parties, including potential merger/acquisition targets.



A framework for response
Identify and evaluate MNPI inflows and outflows.

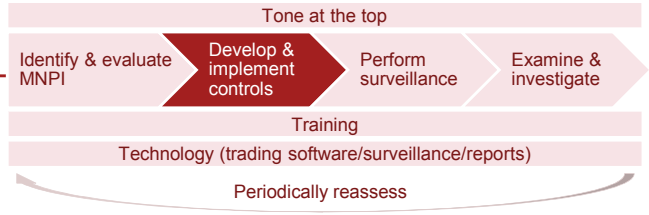
A careful inventory of sources of MNPI should be undertaken in order to fully understand the inflow and outflow of information to/from the firm. The inventory should include information flowing into and out from vendors, third-party providers, companies that are potential merger/acquisition targets, and other sources. The inventory should be reviewed periodically to make sure that important developments have been identified and incorporated.

Sources to consider when generating an MNPI inventory might include:

- Research consultants
- Corporate management with which the firm conducts meetings
- Employees with board seats on outside entities
- Employee-disclosed personal relationships
- Fund investors
- Investment advisers and portfolio companies to which the firm or its employees or principals are economically connected through a firm investment, personal investment, etc.
- Owning different portions of capital structure of issuer
- Former employers of current employees
- Current employers of former employees
- Brokers with whom employees have significant gift and entertainment activity
- Securities transacted around the time of a corporate announcement or that recently had a significant price change around the time of a firm transaction in such an issuer's securities
- Other issuers identified through post-trade surveillance reviews
- Portfolio companies or other third parties that use the firm's physical premises and/or network
- Other advisers that use physical premises and/or network

Top pitfalls:

- *Failing to conduct a meaningful or current inventory of the possible sources of MNPI.*
- *Not identifying high-risk communications.*



A framework for response
Develop and implement MNPI handling controls.

Establish an enterprise-wide control structure to monitor and promote compliance. Rank the possible sources of MNPI according to the risk that each creates for your firm, and tailor your approach to controlling the source based on the risk. For example, higher risks may require more surveillance and monitoring, while lower risks may rely on training and certification.

Some approaches include:

MNPI information flows

- Review controls concerning each source of MNPI in the MNPI inflow/outflow inventory.
- Create, maintain, and monitor information barriers.
- Channel solicitations concerning PIPEs, convertible bond issues, and debt restructurings to appropriate walled-off individuals for evaluation.
- Provide specific controls over high-risk areas, such as the use of "experienced consultants."

Trading activities

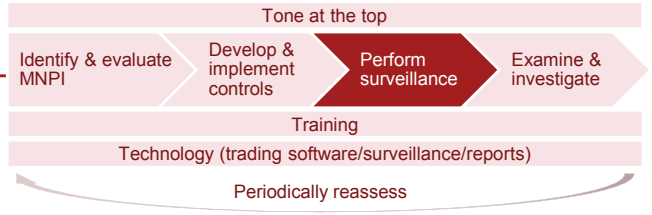
- Use restricted lists, blackout periods, and pre-clearing requirements/procedures for employees based on role and level within the organization.
- Impose controls on blackout/no-trading periods, and/or require employees to pre-clear trades by leveraging technology solutions. Tailor the blackout periods based on event type.
- Require minimum holding periods.

Top pitfalls:

- *Failing to have adequate controls around all possible sources of MNPI.*
- *Training employees, but not having any controls around their handling of MNPI.*

A framework for response

Perform MNPI surveillance and monitoring.



Surveillance should be tailored based on risks specific to the firm and to managers and traders.
Surveillance procedures should be designed to effectively detect potentially incoming or outgoing MNPI, high-risk relationships, compensation provided or received for MNPI, and related trading activity. Results of surveillance procedures should be used to continuously fine tune surveillance efforts.

Some approaches include:

Trading activities

- Review firm trading, client trading, and personal trading activity of employees as part of surveillance activities.
- Perform post-trade surveillance for specific events such as public announcements, price spikes, and profits.
- Assess trades using derivatives that may achieve the same economic effect as a direct trade in the underlying security.

Communi-cations

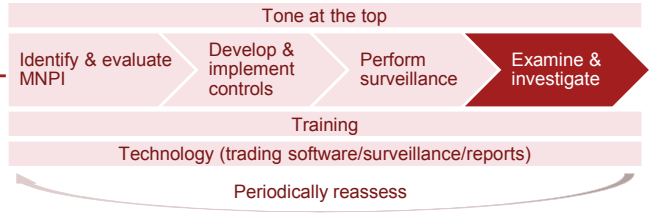
- Perform surveillance for email and other communications about particular stocks for particular employees.
- Perform phone log surveillance to determine with whom employees are speaking.

Top pitfalls:

- *Training employees, but not having any surveillance or controls around their handling of MNPI.*
- *Failing to conduct post-trade surveillance adequately.*
- *Not surveiling high-risk communications.*

A framework for response

Examine trading patterns and investigate anomalies.



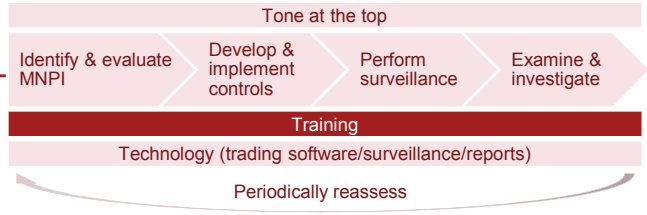
Once surveillance measures are in place, firms should put into place a process for following up and investigating any indication of aberrant trading. Investigations should be conducted to identify whether the trade was made while in possession of MNPI, and action should be taken if the investigation reveals a violation either of the firm's compliance policy or of other policies and procedures.

Key points to keep in mind:

- Investigate any aberrations or exceptions.
- In addition to individual exceptions, be alert to patterns by individuals or in particular units.
- Follow-up should be swift, and consider the "root cause" of problems.
- Timely and thorough investigations are critical, as is the ability to track the results of surveillance activity and investigations.

Top pitfalls:

- *Receiving employee trade reports but not adequately reviewing them.*
- *Failing to follow up on indications of aberrations.*



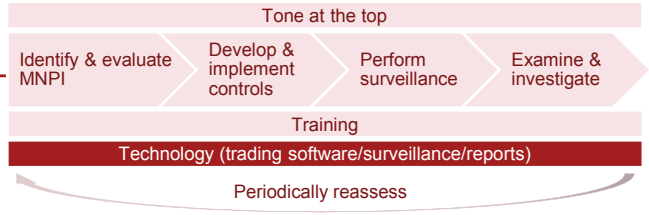
A framework for response
Training

Training is an integral part of a firm's business code of conduct, but should not be generic or one-size-fits-all. Consider whether authority from outside the firm, including former regulators, might better convey the seriousness of the message. Consider an end-of-training assessment that requires employees to achieve a particular score.

Insider trading training	
Promote:	***Training element:***
▪ Overall awareness and understanding	• Identify key terms related to insider trading. Identify rules and regulations governing insider trading, including institution-specific guidelines, responsibilities, obligations, and prohibitions.
▪ Understanding of what applies to each employee and why	▪ To illustrated real-life risks, use situations that your employees encounter.
▪ Understanding of consequences of noncompliance	▪ Use real enforcement cases to demonstrate consequences. Always involve senior management in delivering key messages.
▪ Understanding of gray areas, and how to reach out when the employee has questions.	▪ Use scenario-based situations, based on client-specific examples.

Top pitfalls:

- *Failing to adequately train employees on MNPI.*
- *Employees' belief that certain things do not apply to them or their belief that controls are in place to prevent them from wrongdoing.*



Technology can help leverage surveillance coverage both by restricting the transmission of MNPI and by automating trade review.

Use of technological tools

Information barriers and data security should:

- Create a barrier between MNPI and those people who should not have access.

Electronic communication surveillance should:

- Include testing to identify incoming or outgoing MNPI and patterns and relationships of interest.
- Include firm e-mail, messenger software, Bloomberg, BlackBerry IM, and other Web-based mail and social networking sites used on firm networks.
- Incorporate analysis of telephone logs and calendar entries.

Pre-trade review and approval technologies can:

- Restrict trading activities through order management system (OMS) configuration rules (for example, require additional approvals for trading watch-list securities).
- Simplify employees' personal trading through use of pre-clearance software that scans potential trades against the firm's restricted list, fund trading activity, holding periods, blackout windows, and de minimis thresholds.
- Facilitate testing of trading activity through automated electronic feeds from brokerage firms.

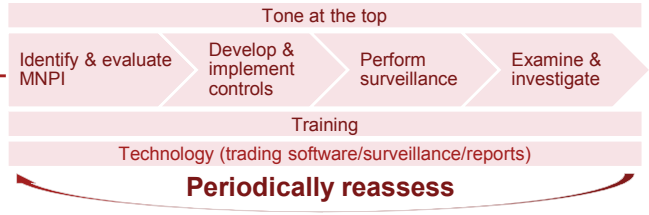
Post-trade surveillance technologies can:

- Identify trading in securities where MNPI may be known.
- Use automated rules or statistical algorithms to identify patterns of trading activity that may indicate the use of MNPI based on multiple risks factors including timing, capital at risk, or performance.
- Incorporate third-party reference data such as news feeds.

Top pitfalls:

- *Failing to understand technological tools available.*
- *Using manual techniques when a technological tool could be more effective and efficient.*

A framework for response
Periodically reassess.



Each facet of the program should be reviewed regularly to make sure that it is functioning effectively. Confirm that:

- Risks are identified and controlled.
- Surveillance and monitoring are effective and efficient.
- The program is adequately capturing the risks, particularly in light of changes to a firm's business or trading strategy, its employees, new surveillance mechanisms, and changes in the law and regulatory expectations.
- Results are being provided to the senior managers responsible for the firm's overall compliance programs and tone at the top.
- Identified deficiencies are being addressed quickly by whatever means necessary (such as updating controls, considering new technological controls and surveillance, incorporating new material into training, or implementing additional testing of trading patterns).

Section 5

How PwC can help

How PwC can help
Client needs and service offerings

Client needs	PwC services	Solutions
Gain greater confidence in existing insider trading program	Targeted review of firm's insider trading program	▪ Review your business processes and flows of information. ▪ Conduct an inventory of sources of MNPI based on firm-specific particular business model and complexity. ▪ Conduct interviews of select employees to identify actual practices and risks. ▪ Review controls around each source, including the monitoring of high-risk communications. ▪ Review effectiveness of restricted and watch lists. ▪ Review surveillance and follow-up practices and procedures, and perform sample testing of the procedures performed. ▪ Review current policies and procedures in light of MNPI source inventory. ▪ To address MNPI issues, review policies and contracts with "expert network" service providers. ▪ Review training materials and methods. ▪ Recommend workable solutions and improvements.
Improve existing programs to prevent and detect insider trading	Targeted review of firm's insider trading program	▪ Provide information on leading industry practices. ▪ Recommend potential changes to controls, policies, and procedures based on our assessment of firm-specific MNPI vulnerabilities. ▪ Recommend potential changes to eliminate sources, to control dissemination, and/or limit the potential misuse of MNPI. ▪ Recommend potential surveillance and monitoring programs to detect trading on MNPI and/or conveying MNPI to others inside or outside the firm in unauthorized manner. ▪ Develop risk-targeted training for your CCO, compliance analysts, internal audit, and other firm personnel on how to identify and investigate suspicious circumstances that may be indicative of insider trading. ▪ Develop recommendations for controlling risks of "expert network" research consultants.

How PwC can help
Client needs and service offerings

Client needs	PwC services	Solutions
Concern about specific information flows or transactions	Special investigations	▪ Conduct special investigations of specific trading patterns, groups, or information flows, often along with outside law firms. ▪ Provide findings and recommendations concerning trading, including possible enhancements to controls.
Assistance in assessing readiness for SEC inspection of firm's insider trading program	Mock exam	▪ Conduct a compliance examination of the firm's insider trading program. ▪ Provide our assessment and recommendations for improvement. ▪ Assess and advise on aspects of the compliance program that might draw attention from the SEC.
An unregistered investment adviser or broker-dealer is preparing to register, and needs a program to prevent and detect insider trading	Registration readiness: assisting organizations in migrating from an unregistered to a registered operating environment	▪ Assist in designing an insider trading program that both addresses regulatory requirements and is tailored to the specific risks at the firm. ▪ Provide training to firm employees about dealing with MNPI and insider trading obligations and prohibitions.
Understand technology solutions	Technology consultation	▪ Assess technology controls related to information barriers and data security. ▪ Benchmark current compliance technology environment, including pre-clearing trades, surveillance and monitoring of portfolio trading, personal trading, and e-communications surveillance. ▪ Advise on the selection and implementation of software solutions. ▪ Develop requirements, and translate the risks of surveillance and monitoring rules used by software. ▪ Test and fine tune surveillance software for efficiency and effectiveness.

How PwC can help

PwC is distinguished by the depth and the breadth of its professionals.

PwC helps market participants to meet the challenges presented by this new reality.

Our teams have significant experience in performing thorough evaluations of risk and compliance programs. PwC can help firms address regulatory compliance issues and effectively manage regulatory risk. Our regulatory team, a part of the firm's national Financial Services Regulatory practice, is comprised of experienced professionals with diverse backgrounds.

Our team includes:

- Former director and an associate director of the SEC's Office of Compliance Inspections and Examinations
- Former associate director of the New York office of the SEC
- Former senior trading specialist
- Former SEC examiners
- Industry-specific experts
- Former chief compliance officers
- Former chief risk officers
- Forensics and investigations experts
- Technology, data, and systems specialists
- Governance, risk, and compliance system providers with which PwC has partnered to offer compliance and control automation

How PwC can help
Our Financial Services Advisory practice

PwC is an adviser to 44 of the world's top 50 banks and 46 of the world's top 50 insurance companies, and is the leading service provider to investment managers, pension funds, and hedge funds around the world. This diverse client base provides us with unique access to develop peer insights and to understand from experience what works in specific client circumstances. In the United States alone, we are able to call upon our 800-person Financial Services Advisory practice and more than 3,000 financial services professionals.

Accountability and cost effectiveness	Our approach to serving our clients provides them with a single point of accountability, which creates an efficient and effective day-to-day working arrangement and, most importantly, best positions our clients for success. We have significant experience in helping to drive complex programs, and believe that we can work successfully in a cost-effective manner to meet your organization's needs and objectives.
Trusted brand	We offer a truly independent view, without prejudice or favor regarding specific vendors, solutions, or approaches. We approach each situation and develop the most appropriate solutions depending upon the client's individual circumstances.
Global footprint	PwC's global footprint benefits clients in terms of consistent service delivery and quality by taking advantage of the best ideas, resources, and solutions from around the world.

How PwC can help

For further information, please contact:

Americas

Lori Richards	lori.richards@us.pwc.com +1 703 610 7513
Tom Biolsi	thomas.biolsi@us.pwc.com +1 646 471 2056
David Sapin	david.sapin@us.pwc.com +1 703 918 1391
A. Duer Meehan	a.duer.meehan@us.pwc.com +1 703 918 6191
Robert Nisi	robert.nisi@us.pwc.com +1 415 498 7169
Anthony Conte	anthony.conte@us.pwc.com +1 646 471-2898

Appendix

Select qualifications

Select qualifications

Large investment bank—Targeted review of potential misuse of MNPI.

Issues	A large investment bank was interested in identifying possible insider trading from a large volume of trading data in response to an SEC enforcement action that cited a failure to maintain and enforce policies to prevent the misuse of MNPI over a five-year period. Given the time and cost constraints associated with a manual exercise of this magnitude, the client wanted to target the reviews by using an automated filtering process. This process was designed to remove from any subsequent manual review those transactions or positions that were not indicative of the potential misuse of MNPI.
Approach	PwC brought together specialists from across the firm to create a team with unique industry and subject-matter expertise. In collaboration with the client, the team conducted an initial analysis of test data to determine the validity of applying statistical modeling for the automated filtering process. The development cycle included: ▪ Conducting pre-model development data analysis to determine the best modeling approach. ▪ Developing statistical models. ▪ Testing the statistical models on hypothetical transactions/positions to determine what types of trading activities would and would not be captured in the model, and adjusting the model accordingly. ▪ Reviewing the model with a third party to make the required adjustments. ▪ Transferring the data back to the client for review. PwC also assisted with the transfer of data from the client to PwC and performed appropriate validation and data cleaning, when necessary. For those cases flagged by the automated filtering process, a second team of PwC Financial Services resources performed extensive manual reviews to assess whether there were transactions characteristic of the potential misuse of MNPI. As the manual process proceeded, additional filtering processes were developed and implemented to minimize both false positives and false negatives.
Benefits	Working with PwC, the client satisfied the SEC's requirement. Furthermore, the number of cases that required manual review at the client was reduced. This resulted in substantial cost savings to the client while providing credible and defensible results.

Select qualifications

$12 billion investment management firm with a public trading unit—Gap analysis comparing existing insider trading policy to Advisers Act requirements.

Issues	An investment management firm with a public trading unit had only a rudimentary policy in place concerning MNPI—one that had not been substantially updated for years.
Approach	PwC performed a gap analysis comparing the existing policy to Advisers Act requirements, regulator expectations, and peer best practices. The gap analysis identified deficient areas of the policy, and recommended procedures for curing them.
Benefits	Among the recommendations for the adviser were: ▪ Establishing a procedure for making an inventory of sources of MNPI. ▪ Creating a protocol by which employees were required to report receipt of MNPI. ▪ Creating watch lists, restricted lists, and information barriers to control information flows. ▪ Inventorying nondisclosure and confidentiality agreements on an ongoing basis, and assessing them as sources of flows of MNPI. ▪ Requiring additional disclosure of employee relationships and outside business activities to assist in the inventorying of sources of MNPI.

Select qualifications

Large hedge fund adviser—Surveillance and monitoring protocols to detect and deter trading while in possession of MNPI.

Issues	A hedge fund adviser with multiple sites, outside relationships, and investment management personnel sought to create surveillance and monitoring protocols to detect and deter trading while in possession of MNPI.
Approach	Based on an inventory of potential sources of MNPI (such as research consultants, strategic investors, employee relationships, and other investment advisers in which employees had economic ties), PwC recommended a series of specific tests and the monitoring of electronic communications, as well as tailored post-trade surveillance.
Benefits	PwC's recommendations gave the firm's compliance function an opportunity to reduce "false positive" testing results and to target surveillance at high-risk relationships and trading activity.

Select qualifications

Financial services firm–Investigation of allegations of misuse of MNPI.

Issues	PwC was engaged by outside counsel and senior management at a large reinsurance carrier to investigate a whistleblower allegation relating to the misuse of MNPI by several key executives.
Approach	The analysis included identification of the sources of MNPI and related policies, controls, and technology to prevent and detect the misuse of MNPI. The analysis also involved testing electronic trading data for potential misuse of MNPI, and testing emails and electronic communications using a targeted keyword list. The investigation included identifying potentially suspicious trades and interviewing key parties involved in these transactions. Specific analyses pertaining to the identification of potential misuse of MNPI included: ▪ Developing an inventory of securities where MNPI may have been known, based upon watch list, restricted list, private equity deals, employee disclosures, and other sources of information. ▪ Testing electronic firm and personal trading data for securities included in the inventory of securities where MNPI may have been known. ▪ Testing electronic trading data for compliance with blackout period restrictions and holding periods. ▪ Developing and applying algorithms to identify trading patterns indicative of the potential misuse of MNPI, based upon such factors as timing, size, and performance of trades. ▪ Developing targeted, risk-based keyword lists for email searches. ▪ Analyzing the potential usage of expert networks, including phone logs, email keywords, and related trading activity.
Benefits	Our report was prepared in conjunction with outside counsel and presented to senior management to help them evaluate the claims made in the whistleblower letter regarding the potential misuse of MNPI. In addition, PwC provided observations and recommendations related to policies and controls to prevent and detect the possible future misuse of MNPI.

www.pwc.com

“Avoiding the Headlines: How Financial Services Firms Can Implement Programs to Prevent Insider Trading,” PwC FS Viewpoint, June 2011. www.pwc.com/fsi