

RISK, RULES AND COMPLIANCE

How to Combat Insider Trading and Manage Enforcement Priorities

TABLE OF CONTENTS

- 1 Executive Summary
- 1 ASIC on Insider Trading and Market Manipulation
- 2 Key Australian Rules and Regulations
- 3 Current Consultation Papers in the Market Place
- 3 Role of Professional Organisations Supporting the Financial Industry
- 4 Why Use an Automated Compliance System
- 4 The Challenges of Implementing Employee-facing Compliance Programs
- 5 The Optimal Solution to Meet the Challenges
- 6 Conclusion

EXECUTIVE SUMMARY

As regulators around the world put more pressure on companies to tighten their corporate governance mandates, many financial organisations are looking aggressively for ways to control costs while also meeting regulatory requirements. The Asia-Pacific region, therefore, is also feeling the heat to ramp up its implementation and management of efficient personal trading compliance practices.

On 1 August 2010, the Australian Securities and Investments Commission (ASIC) took over the supervision of trading on Australia's domestic licensed markets and its trading participants from the Australian Securities Exchange (ASX). While the ASX will still be responsible for supervising listed companies, ASIC and the Corporations Act will ensure that companies manage potential conflicts of interest, such as insider trading and market manipulation which may occur as a result of employee activities. ASIC will be responsible for the supervision of domestic licensed financial markets and its participants.

According to the ASX Markets Supervision annual report, there has been an increase in insider trading claims and evidence of market manipulation as markets have become easier to access, thanks to the emergence of complex products. The ASX reported over 90 cases of market manipulations from January 2009 to first quarter 2010.¹

To effectively manage growing regulatory challenges, financial organisations must first understand what is being required of them from the regulators and take the appropriate steps to mitigate regulatory, operational and reputational risks. The optimal solution to these challenges will include leveraging trusted compliance expertise and utilising an automated employee-facing compliance solution.

ASIC ON INSIDER TRADING AND MARKET MANIPULATION

In his speech on 13 August 2010, Tony D'Aloisio, ASIC's Chairman, indicated strongly that ASIC will be stepping up the detection, investigation and enforcement of insider trading and market manipulation related cases. He also highlighted recent enforcement matters and emphasised ASIC's serious intent and determination to prosecute wrongdoers in order to preserve public confidence in the market's integrity.²

ASIC currently has 69 enforcement matters relating to market integrity and, since 1 January 2009, it has had 16 significant outcomes relating specifically to insider trading and market manipulation, including:

- four outcomes – three convictions and one guilty plea – for insider trading (Panchal, O'Reilly, Stephenson and Hartman);
- five outcomes – four convictions and one civil penalty – for market manipulation (Wade, Musumeci, Newing, Soust and Chan); and
- the banning of seven brokers from providing financial services, for having engaged in either insider trading or market manipulation.

In addition, they have another eight insider trading and market manipulation matters pending before the court, on possible criminal charges.

Moving forward, the industry can expect ASIC to take a much more dominant and aggressive approach towards regulating insider trading and market manipulation, in order to meet world leading standards set by the Securities and Exchange Commission (SEC) in the United States and the Financial Services Authority (FSA) in the United Kingdom, for example.

¹ ASX Markets Supervision (ASXMS) Quarterly Activity Report, March 2010. http://www.asx.com.au/about/pdf/asxms_quarterly_report_mar2010.pdf

² Tony D'Aloisio, 13 August 2010. [http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/speech-insider-trading-market-manipulation-August-2010.pdf/\\$file/speech-insider-trading-market-manipulation-August-2010.pdf](http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/speech-insider-trading-market-manipulation-August-2010.pdf/$file/speech-insider-trading-market-manipulation-August-2010.pdf)

KEY AUSTRALIAN RULES AND REGULATIONS

The following are a few important highlights of the tightened regulations, as set forth by ASIC and ASX.

Corporations Act 2001 Part 7.10 – Market Misconduct and Other Prohibited Conduct Relating to Financial Products and Financial Services³

The Corporations Act 2001 Part 7.10 provides details of what is considered unethical behaviour by participants in the finance industry. For example, a person must not take part in market manipulation, insider trading or any prohibited conduct which does not promote an “honest” and “fair” market place. Such unethical behaviour may result in civil or criminal actions taken against an individual or company.

The Corporations Act 2001 Part 7.10 requires investment companies to manage potential issues that may occur as a result of their employees’ access to material non-public information. Employees with such access are known as covered/access persons, and it is the company’s responsibility to implement steps to ensure that employees’ actions are ethical by implementing requirements such as insider lists, trade pre-approval and director disclosures.

ASIC Regulatory Guideline 79 – Managing Conflicts of Interest: A Guide for Research Report Providers⁴

The ASIC Regulatory Guideline 79 addresses licensees who are Research Report Providers (also known as research analysts, securities analysts or research houses). If they or their research staff trade in the financial products that they actively research, there may be a potential conflict of interest. As a result, organisations must take steps to ensure the integrity of research reports is not compromised.

ASIC Regulatory Guideline 181 – Licensing: Managing Conflicts of Interest⁵

The ASIC Regulatory Guideline 181 Licensing is a conflicts management obligation that requires Australian Financial Services Licence (AFSL) holders to have sufficient processes in place to manage conflicts of interest. As disclosure alone is inadequate, companies need to implement and follow these three identified mechanisms of controlling, avoiding and disclosing conflicts:

- (a) identify the conflicts of interest relating to their business
- (b) assess and evaluate these conflicts
- (c) decide upon and implement an appropriate response to these conflicts

ASIC Regulatory Guideline 193 – Notification of Directors’ Interests in Securities – Listed Companies⁶

Section 205G(1) of the Corporations Act 2001 requires every director of an Australian listed public company to notify the relevant market operator (i.e. the operator of the market in which the company is listed) of:

- (a) the director’s relevant interests in securities of the company or a related body corporate
- (b) contracts
 - (i) to which the director is a party or under which the director is entitled to a benefit; and
 - (ii) that confers a right to call for or deliver shares in, debentures of, or interests in a managed investment scheme made available by, the company or a related body corporate

³ Corporations Act 2001. http://www.austlii.edu.au/au/legis/cth/num_act/ca2001172/

⁴ Regulatory Guideline 79 – Managing Conflicts Of Interest: A Guide for Research Report Providers. Australian Securities & Investments Commission. November 2004. [http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/managing_conflicts_interest_guide.pdf/\\$file/managing_conflicts_interest_guide.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/managing_conflicts_interest_guide.pdf/$file/managing_conflicts_interest_guide.pdf)

⁵ Regulatory Guideline 181 – Licensing: Managing Conflicts of Interest. Australian Securities & Investments Commission. 30 August 2004. [http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/ps181.pdf/\\$file/ps181.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/ps181.pdf/$file/ps181.pdf)

⁶ Regulatory Guideline 193 – Notification of Directors’ Interests in Securities – Listed Companies. Australian Securities & Investments Commission. June 2008. [http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/rg193.pdf/\\$file/rg193.pdf](http://www.asic.gov.au/asic/pdf/lib.nsf/LookupByFileName/rg193.pdf/$file/rg193.pdf)

As directors have access to significantly more detailed information about their companies than their shareholders, the latter may be influenced by actions taken by directors in relation to the acquisition or disposal of shares. Together with the insider trading and market manipulation regulations, RG 193 aids in enforcing an informed and orderly market.

The ASX Listing Rule 3.19A⁷ is a complementary requirement to Section 205G. It requires disclosure by the company of certain interests in securities held by directors, together with some additional information, within five business days of the relevant change occurring (see RG 193.17).

CURRENT CONSULTATION PAPERS IN THE MARKET PLACE

Consultation Paper 128 – Handling Confidential Information⁸

The Consultation Paper 128 is a draft regulatory guide developed by ASIC that presents best practice guidelines for listed companies, their advisers and other service providers. The Paper discusses the significance of handling and controlling confidential information and highlights market practices that may reduce the risk of insider trading and non-compliant activities. To address the suggested guidelines, companies should implement a policy to regulate confidentiality and personal trading by employees.

The paper requires companies to maintain a register of both internal and external parties who are insiders on sensitive transactions. Employment contracts should also explicitly include the employer's right to access all communication records including email, phone records and broker communications in efforts to monitor any potential insider trading activity. Employees with confidential information will also be required to obtain pre-approval from the company before trading in any restricted securities and perform post-trade analysis of executed trades using copies of contract notes directly from the employee's broker maintained by compliance personnel.

Recommendation 3.2 of the ASX Corporate Governance Principles and Recommendations⁹ also states that companies should have a policy in place concerning trading in company securities by directors, senior executives and employees. As a primary rule, companies should restrict trading by staff that may have inside information about the company's own securities. ASX is consulting on a proposal to introduce a new Listing Rule that requires companies to adopt a trading policy that identifies the periods of the year when trading by key management personnel should be restricted, with the exception of certain circumstances. It may be practicable for larger organisations, particularly in the financial services industry, to have a computer compliance system that tracks, audits and oversees employees' securities transactions.

ROLE OF PROFESSIONAL ORGANISATIONS SUPPORTING THE FINANCIAL INDUSTRY

Various professional organisations serving the Australian Industry, like the Financial Planning Association (FP), the Investment and Financial Services Association Limited (IFSA) and the Australian Financial Markets Association (AFMA) also recommend codes of ethics and rules for professional conduct. Their guidelines help prevent illegal insider trading and market manipulation.

⁷ Disclosure of Directors' Interests, AFX Listing Rule 3.19A. Australian Securities Exchange. January 2003. <http://www.asx.net.au/ListingRules/chapters/Chapter3.pdf>

⁸ Consultation Paper 128 – Handling Confidential Information. Australian Securities & Investments Commission. 21 December 2009. <http://www.asic.gov.au/asic/asic.nsf/byheadline/09-264AD+ASIC+releases+new+best+practice+proposals+for+the+handling+of+confidential+information+and+conduct+of+market+soundings?openDocument>

⁹ Guidance Note 9A: Recommendation 3.2. Corporate Governance – Principles and Recommendations. Australian Securities Exchange. http://www.asx.net.au/ListingRules/guidance/gn09a_corporate_governance_principles.pdf

WHY USE AN AUTOMATED COMPLIANCE SYSTEM?

Regulatory compliance in the financial services industry is vital as many risks can arise in companies due to conflicts of interest from their employees' related activities. Companies that perceive regulatory obligations to be more of a nuisance than a benefit place themselves at financial and reputational risk. Regulation exists to uphold and maintain the integrity of the industry and manage these conflicts and a compliance system helps companies meet their regulatory compliance responsibilities by helping to reduce operational costs associated with risk exposure. The consequences of unmanaged risk can be greater than fines imposed by any regulatory body as a company's reputation can be damaged irrevocably. Furthermore, the collapse of organisations such as Storm Financial and Opes Prime in Australia are sobering reminders of the crucial role an effective employee-facing compliance program plays in the financial services industry.

THE CHALLENGES OF IMPLEMENTING EMPLOYEE-FACING COMPLIANCE PROGRAMS

It is not easy to implement a good employee-facing compliance program that is cost-effective and yet meets regulatory requirements. The challenges can be divided into two distinct areas: Information Gathering and Information Analysis.

Information Gathering

Information gathering requires a company to analyse and manage the information received from the sources of potential employee conflicts of interest, such as paper-based processes, email communications and phone conversations.

Companies that require employees to obtain clearance prior to personal trading typically have a separate system or process to manage the request. This process might be initiated via the submission of a paper-based form, an informal email and/or a phone call. The request is then routed to the individual's manager to ensure that there is no conflict of interest or other issues as a result of trade execution. Each individual involved in the approval process may use particular information, such as a restricted list, to determine and identify any issues. As the required analysis can often be extensive and time consuming, these individuals may circumvent the appropriate checks. Also, once the request is approved or denied, the evidence of the final outcome is usually kept in a spreadsheet, an email or filed with the employee's record, making retrieval of the information cumbersome.

The administration of employee annual or quarterly certifications/attestations is equally cumbersome. Identifying which attestations are required from which employees and the necessary tracking of responses all add up to an arduous process. Once again, compliance resources are diverted from more critical concerns to tedious administrative details, resulting in efforts that are more intensive than necessary.

Typically, other potential sources of employee conflicts of interests, such as the tracking of gifts and entertainment expenses, are kept separate from an employee's personal trading records. This leads to disjointed systems which further complicate the information gathering process and prevent a company-wide view of risk.

Information Analysis

Information analysis suffers as a direct result of information gathering complications. Due to the considerable time and effort spent on the latter, little attention is therefore given to proper analysis. For example, the identifying of issues related to employee personal trading is minimised to only basic cursory checks. This is because all the relevant information is housed in disparate systems in various formats representing employee trades.

This constraint impedes a company's efforts to identify broader issues and increases the likelihood of errors. Forensic testing is only feasible for a small percentage of the information, due to the sheer volume of information available for analysis. As a result, in addition to being non-compliant, a company incapacitated by these limitations is open to regulatory scrutiny and, potentially, fines.

Many companies fail to maintain a sound employee-facing compliance program because of its manual and time-consuming nature. In addition, an inability to keep current with new regulations and interpretations, as well as company policy changes, eventually leads to premature program obsolescence. There is frequently a slow and ineffective response to internal or external audits, leading the company to become systematically exposed to risks resulting from employee-related activities.

THE OPTIMAL SOLUTION TO MEET THE CHALLENGES

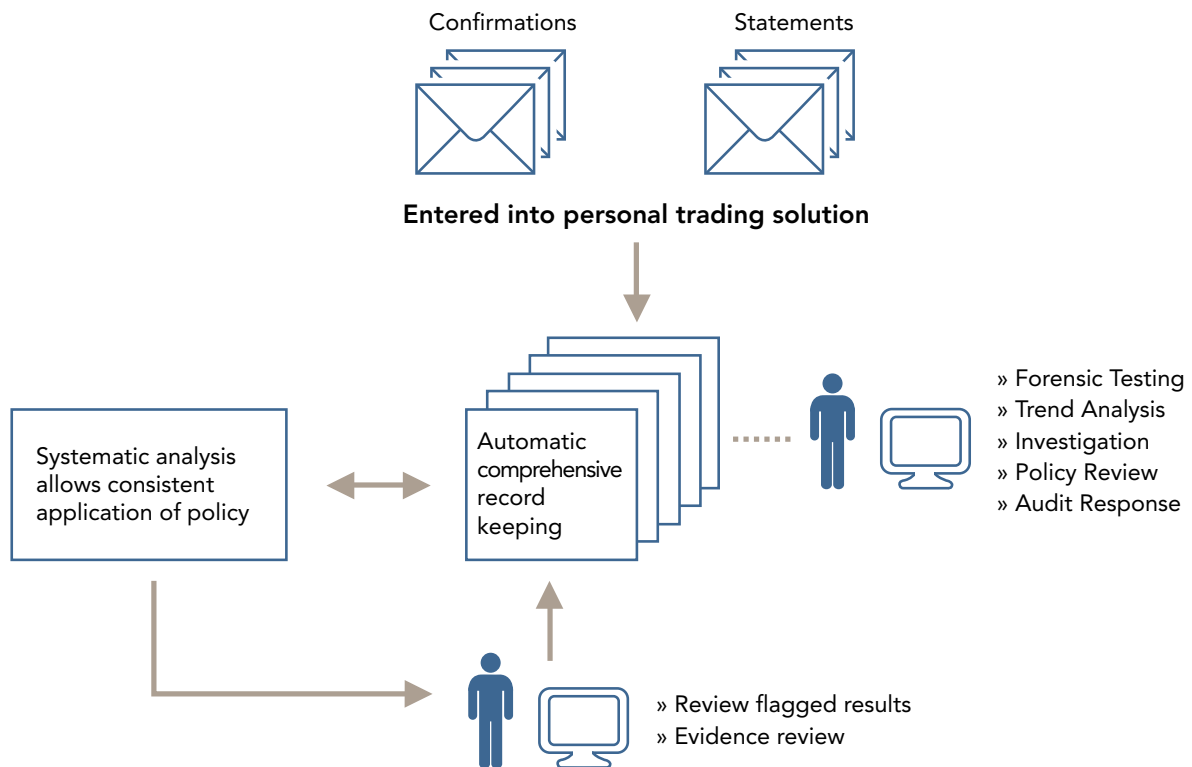
An optimal employee-facing compliance solution comprises features designed to address several key factors.

User-friendly Interface

A simplified end-user application encourages employees to adhere to business compliance requirements. An easy interface allows the end user to complete the necessary transactions quickly, whether it is responding to an attestation or submitting a trade pre-clearance request.

Optimal Pre-approval Process Picture

Streamlined information gathering and analysis:



Centralisation

Centralisation of information is crucial to a proper employee-facing compliance solution. This simplifies the overall burden by collecting and collating all the information which is normally maintained across different systems.

Best Practices

The use of industry-wide best practices extends a company's capabilities and harnesses the knowledge belonging to peer companies. This enables corporations to quickly respond to regulatory changes, as well as tap into a market-wide analysis of regulatory requirements. In addition, a solution which accommodates numerous compliance practices allows a company to remain consistent with shifts in the compliance landscape without the need for a complete overhaul of the program.

Enhanced Reporting Capabilities

Highly flexible and complete reporting capabilities enable companies to quickly retrieve information collected within the solution. This allows companies to appropriately respond to enquiries and audits and facilitates forensic testing and investigations as well.

Automation

Due to the large amount of applicable information available for analysis, an automated review of data is an absolute necessity. Therefore, an effective solution should be able to systematically cross-examine all relevant data to determine potential breaches in regulations and ensure the consistent application of company policy. This is particularly true of employee personal trading where the surveillance of market manipulation and other trade-related issues requires a lot of effort. Shifting this burden from compliance resources allows companies to focus on issues that require more scrutiny and forensic testing.

CONCLUSION

The increasing regulatory obligations of financial services companies in Australia and New Zealand, coupled with the potential reputational and financial risks involved with non-compliance, are strong arguments for companies to implement an effective employee-facing compliance program to promote sound business practices.

Information gathering and information analysis present obstacles because of the manual and time-consuming nature of the work involved. Companies are therefore left with a mass of information without the proper means to effectively manage the exposure from unknown risks associated with them. In addition, with employees perceiving their obligations as undue burdens, an overly complicated system only encourages them to evade the process.

The appropriate employee-facing compliance solution provides companies with the ability to meet the regulatory requirements while effectively managing the challenges that come with them. Automated Information Gathering offers a centralised and comprehensive single view of information, allowing for thorough forensic testing and investigation. The optimal solution also simplifies compliance work flows to ensure that employees adhere to policies.

Knowledge of industry best practices allows forward-thinking compliance programs to incorporate improvements based on the experience of peer or related companies. The company therefore benefits from the collective experience of the industry as a whole.

Although implementing a solution in itself serves as evidence of a company's sincerity towards its regulatory responsibilities, the solution must also be customised to address the needs of the company.

About SunGard's Protegent

SunGard's Protegent solutions for compliance, suitability and new account opening help retail and institutional investment firms oversee business processes relating to compensation management, client acquisition and suitability, as well as employees' personal trading and code of ethics, while helping reduce expenses and address regulatory requirements. Protegent supports compensation management, supervision and surveillance practice, helps streamline the compliance life cycle, proactively monitors trades and provides comprehensive auditing and reporting for financial institutions and companies that trade in energy and commodities markets.

About SunGard

SunGard is one of the world's leading software and technology services companies. SunGard has more than 20,000 employees and serves 25,000 customers in 70 countries. SunGard provides software and processing solutions for financial services, higher education and the public sector. SunGard also provides disaster recovery services, managed IT services, information availability consulting services and business continuity management software. With annual revenue exceeding \$5 billion, SunGard is ranked 380 on the Fortune 500 and is the largest privately held business software and IT services company.

For more information, please visit www.sungard.com.

www.sungard.com/protegent

SunGard Protegent Australia
Lv 11, 115 Pitt Street
Sydney, Australia
Tel: (+61) 02 8236 9300
Fax: (+61) 02 8236 9399

General Inquiries:
trading-info@sungard.com

SunGard Protegent Singapore
71 Robinson Road
#15-01
Singapore 068895
Tel: (+65) 6308 8000

©2010 SunGard.

Trademark Information: SunGard, the SunGard logo and Protegent are trademarks or registered trademarks of SunGard Data Systems Inc. or its subsidiaries in the U.S. and other countries. All other trade names are trademarks or registered trademarks of their respective holders.