MCO
MyComplianceOffice

Mitigating Employee Conflicts of Interest

in Financial Services

Table of Contents

Introduction

What is the potential cost of conflicts of interest? Regulators around the globe are cracking down on financial firm employees engaging in unethical and unlawful actions, with hefty fines and harsh penalties imposed.

Beyond the individual impacts, regulators have taken aim at firms acting in conflict to their customers' best interests. For example, on 31 October 2024, the US Securities and Exchange Commission (SEC) charged two securities and investment management firms found to have made misleading disclosures to brokerage customers who invested in its "Conduit" private funds products[1]. Customer funds were pooled and invested in private equity or hedge funds that would later distribute to the Conduit private funds shares of companies that went public. As a result, investors were subject to market risk, with the value of certain shares declining significantly as shares took months to sell. Sanjay Wadhwa, Acting Director of the SEC's Division of Enforcement, notes that, "Conduct across multiple business lines violated various laws designed to protect investors from the risks of self-dealing and conflicts of interest."

On 25 January 2025, Hong Kong's Securities and Futures Commission (SFC) also reprimanded and fined a major bank HK$66.4 million for serious failures in selling investment products, including inadequate disclosure of monetary benefits[2]. While most transactions were declared as the client's "own choice", the firm's relationship managers had influenced 46 clients through solicitation or recommendation of trades. The clients were advised into conducting excessively frequent transactions with short holding periods, a trading pattern which contradicted both the funds' investment objectives and the clients' preferred investment horizons. The SFC found the firm failed to avoid conflicts and to treat clients fairly.

News releases into high-profile cases such as these can cause serious damage to firms' reputation, erode client trust, and put future business opportunities at risk.

This eBook will explore a range of conflicts of interest and how you can minimise the risk of severe penalties, reputational damage, and enforcement actions against your firm and its people.

The State of Enforcements Across the Globe

United States

In fiscal year 2024 (October 1, 2023 to September 30, 2024), the SEC filed 583 enforcement actions[3]. Although down 26 % from the prior year, the US regulator secured a record-high US $8.2 billion in financial remedies (comprising US $6.1 billion in disgorgement and interest and US $2.1 billion in civil penalties). Additionally, the SEC obtained orders barring 124 individuals from serving as officers and directors of public companies, the second-highest number of such bars obtained in a decade.

United Kingdom

In the 2024 calendar year, the UK Financial Conduct Authority (FCA) issued 25 fines totalling £176 million[4]. Prominent outcomes included multi-million-pound penalties in retail and investment banking and the audit sector, reflecting failings ranging from a lack of systems and controls to listing-rule disclosure breaches. The FCA also sanctioned a number of individuals, with penalties and prohibitions for misconduct including closed-period dealing and integrity failings.

Australia

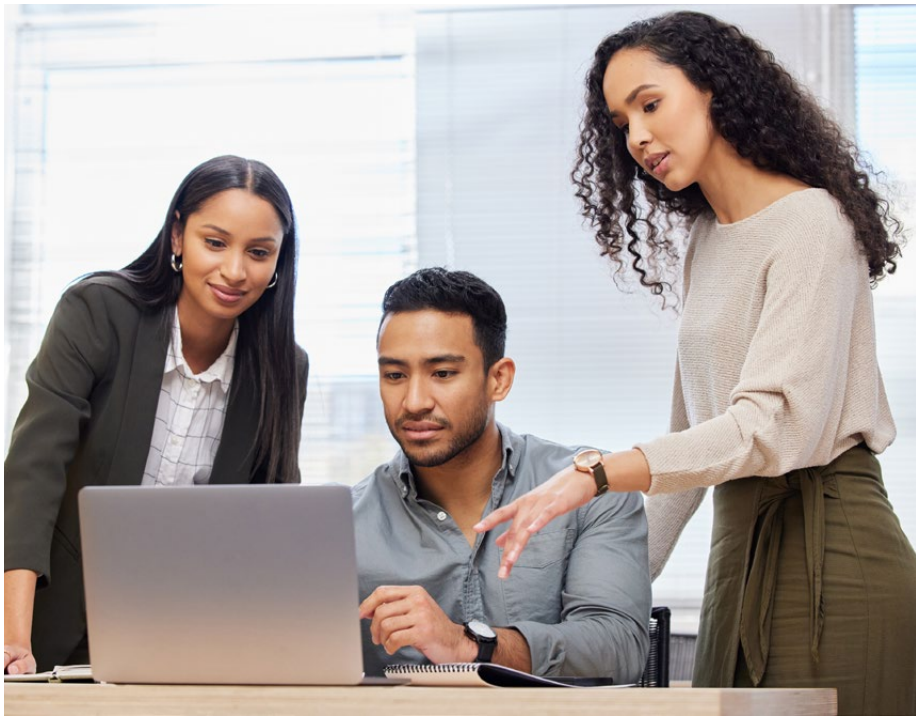
During Australia's financial year FY24-FY25, ASIC obtained AUD $104.1 million in civil penalties, commenced 38 civil proceedings, and worked with the Commonwealth Director of Public Prosecutions (CDPP) to see 24 individuals charged with 128 criminal charges[5]. In addition, the regulator removed or restricted 89 individuals from providing financial services or credit and disqualified 15 company directors.

Enforcement Actions

The stakes are high for firms and their employees and senior management to avoid conflicts and uphold regulatory obligations.

Regulators can trigger enforcement actions across a range of areas, including:

- **Insider trading** and market abuse.
- The use of material non-public information **(MNPI)** for personal and financial gain.
- **Misconduct** involving misleading behaviours related to greenwashing and crypto investments.
- Predatory **financial lending** practices.
- Failure to **deliver value** to investment fund members due to conflicts of interest.
- Misconduct around **misinformation** of financial products and services, particularly throughout advertising and social media vehicles.
- **Unethical behaviours** related to professional education courses and certifications.



Financial institutions (FIs) have direct influence and responsibilities over fund management and financial outcomes for consumers. As such, they are also at heightened risk of individuals using the information and resources of their organisations for personal and professional gains.

Regulatory authorities are put in place to protect investors against harmful activities, hold wrongdoers accountable, deter future misconduct, and maintain the integrity of the financial services industry. But it is imperative that Compliance Officers, Chief Compliance Officers, and other key personnel can identify, monitor, and act appropriately on any red flags and conflicts of interest that may result in unethical and unlawful behaviours.

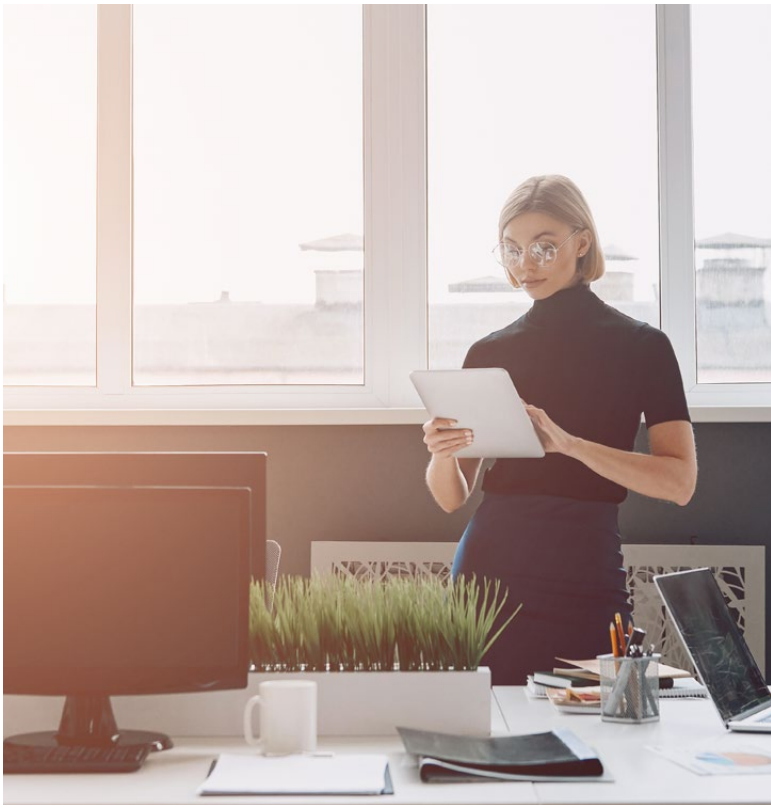
Understanding Conflicts of Interest

A conflict of interest arises when an individual has a personal or financial interest that interferes (or appears to interfere) with their ability to make impartial decisions. But why do these conflicts occur? It comes down to personal gain.

Many brokers and financial advisors see significant income benefits through commission-based compensation, which can create a conflict between what is best for the financial agent and their customer. Employees, executives and directors may also act on sensitive or confidential information to which they are privy to drive better financial outcomes for themselves or their company, again creating a conflict between personal interests and what is best for the integrity of the broader financial market.

More potential conflicts arise when looking at OBAs (outside business activities) where work is being undertaken for multiple employers simultaneously, and GEH (gifts, entertainment, and hospitality) comes into question. Some of these risk areas seem benign at first. They can, however, result in serious repercussions, including job losses, monetary penalties, and reputational damage.

Personal Relationships



Close personal relationships can sometimes influence (or be perceived to influence) the decisions of employees, executives, and directors alike. These relationships can also result in exposure to MNPI that may not have otherwise occurred. Therefore, disclosure of these relationships is critical to helping compliance teams monitor and avoid conflicts of interest.

Even when personal relationships have not resulted in favouritism, unfair advantage, or financial gain, failures to disclose those relationships can create the perception that there may be something to hide. To maintain the trust of all employees, clients, and stakeholders, have robust processes in place to see that:

- **Definitions** of personal relationships that need to be declared are clear and easily understood by employees.
- Employees receive proper **communications and dissemination** of your policies and processes.
- You provide **training and support** to help employees understand the ethical implications of leveraging personal relationships for personal or professional gains.
- Personal relationship policies are included in **attestations** to document that employees acknowledge and understand their obligations.
- Employees have a clear process for **declaring connected persons** and relationships.
- You have a system to **monitor** and confirm that employees are meeting obligations.

Financial firms that effectively manage the disclosure of personal relationships can significantly reduce conflict of interest risk and maintain the trust and confidence of their clients and the public. And while record-keeping can be challenging, especially for large firms with thousands of employees, automated compliance management software can streamline the process, tracking compliance and flagging potential areas of risk.

Attestation Best Practices

Compliance attestations confirm that employees have received current information and training on the policies and procedures with which they must comply. Attestations also ensure they have read and understood those policies and are willing and able to meet the required standards.

New Employees and Employee Onboarding

When new employees start at your firm, they should declare any existing securities they hold. This process enables compliance teams to evaluate any potential conflicts of interest, particularly those arising from MNPI available to the employee, which may impact their roles or trading of securities.

A proper employee onboarding attestation process will also ask staff to attest to their willingness to comply with all relevant policies in the firm, including personal trade policies. These attestations confirm that employees have received, read, and understood policy information and training and can comply with policy requirements.

Ongoing Attestation

Annual re-attestation or certification of employees' trading accounts (and potentially those of their close personal relationships) should also be undertaken to identify any changes and confirm the details they have provided are true, accurate and complete.

Putting the Spotlight on Moonlighting

Outside Business Activity (OBA) is where employees undertake work other than what they produce for their primary employer under contract, aka 'moonlighting' or a 'side hustle'. Particularly following the global pandemic which brought rapid financial uncertainty for many employees, moonlighting moved even more into the spotlight.

According to an Express Employment Professionals-Harris Poll, nearly 90 % of US job seekers have worked a side hustle, with 41 % admitting to doing so during company time, either part time or full time[7]. The most common reasons employees cited moonlighting during company time were to earn extra money to increase savings (59 %) and cover expenses (51 %).

90 %
of US job seekers have worked a side hustle

41 %
admit to doing so during company time

However, when employees fail to communicate their moonlighting activities to their employers, conflicts of interest can arise. Without visibility of those OBAs, firms are severely limited in their capacity to identify conflicts and prevent them from becoming larger issues.

While multiple employment activities are common, they must still be evaluated to determine if potential conflicts exist. Directors may sit on several boards, for example, and employees may help out in family businesses from time to time. Firms can avoid conflicts, however, with policies around the disclosure, evaluation, and approval or denial of OBAs.

To more effectively manage OBAs and reduce risk to your financial firm, ensure you have the following:

- **Defined policies** that address your firm's requirements and processes around OBAs. Consider whether some OBAs can be automatically approved, or if others should be automatically denied.
- **Strong communication** of your documented OBA policies to all employees.
- A **company culture** of talking openly about potential conflicts of interest and how to avoid them.
- **Regular reporting and attestation** of OBAs to identify new or changed activity that should be flagged.
- The **regulatory technology (RegTech)** to automate OBA processes and reporting, and enable employees to easily declare any potential outside business activities and interests.

RegTech can help compliance teams of all sizes more effectively manage OBAs with far less time and effort than manual management.

MCO's award-winning RegTech suite enables pre-clearance of various OBAs, including directorships, contracts and voluntary positions. Configurable workflows can also be created for each type of Outside Business Activity with multiple approval levels, and escalation of requests based on hierarchy. Additionally, OBAs can be embedded into standard attestation questionnaires to reduce barriers to keeping OBAs updated.

Learn more about how a leading-edge RegTech solution can do the heavy lifting for small compliance departments needing a better way to manage OBAs.

Gifts, Entertainment, and Hospitality

Compliance teams must maintain a focus on implementing robust policies and procedures that identify and collate any gifts received or given by employees to clients or counterparties.

Clarity within those policies and procedures is also essential in driving the proper outcomes. For example, if an employee invites a client to an event, it's considered entertainment, whereas an employee giving event tickets to a client is a gift.

Your policies and other critical actions taken as part of your processes should include the following:

- **Clear differentiation** of activities that helps employees better understand gifts and entertainment policies.
- Maintenance of a **central register** to make it easy to declare and track all activities.
- **Periodic reviews** of gifts and entertainment records to detect any irregularities or policy breaches.

MCO's Gift, Entertainment and Hospitality is a comprehensive solution for monitoring employee gifts, meals, entertainment, travel and hospitality activities, allowing firms to record and detect risk within declared gifts and entertainment. It will enable your firm's policies to be embedded with a rules-based approach to identifying potential misconduct and bribery risk.

Download your Gifts, Entertainment, and Hospitality Compliance brochure for more information.

Communications Surveillance

Electronic communications (eComms) messages occurring outside of approved, recorded systems, have gained an increasing share of the regulatory spotlight in the UK, US, Europe, and the APAC region in recent years. Regulators now expect evidence—not only of detection but also of behavioural change driven by strong policies, oversight and regulatory technology (RegTech).

All conversations that involve business communications typically need to be captured, particularly when using firm-issued devices to detect and record conflicts of interest. Firms often record business-related calls and messages on both firm-owned devices and, in some cases, personal devices used under a Bring Your Own Device (BYOD) policy. Regulatory requirements around conversation capture vary by firm and operating jurisdiction, but tend to focus on communications with clients, transaction orders, or any discussions that could impact market integrity.

In the Asia Pacific region, the prevalence of so-called "super-apps" such as WeChat presents further complexity. These platforms integrate messaging, payments, social media and other services into a single ecosystem, making them widely used for both personal and business interactions. For surveillance teams, this creates significant challenges in distinguishing professional communications from personal use and ensuring that all relevant records are effectively captured.

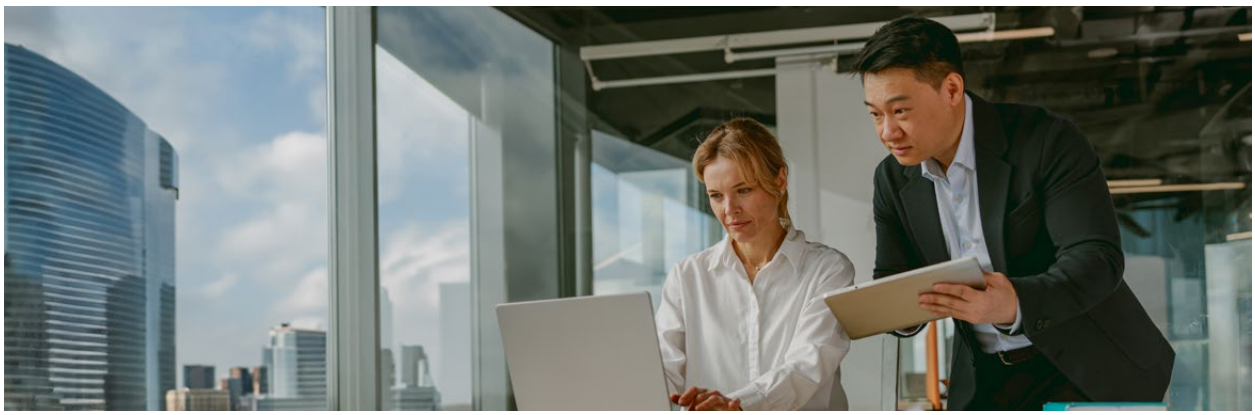
As an authority at the forefront of eComms regulation, the UK's Financial Conduct Authority (FCA) released findings on 07 August 2025 detailing its review of firms' management of off-channel communications[8]. The review highlighted that while most financial institutions (FIs) surveyed strengthened their frameworks, breaches have happened across all staff levels. More alarmingly, 41 % of these breaches involved director-level roles and above. The FCA reaffirms that "Robust record-keeping and monitoring of communications is essential for firms to detect and investigate misconduct."

41 %
of eComms breaches reviewed by the FCA involve director-level roles and above

In Australia, ASIC has released Information Sheet 283[9], which warns that unmonitored encrypted channels create a heightened risk of misconduct going undetected. Similarly, the Monetary Authority of Singapore (MAS) and Hong Kong's Securities and Futures Commission (SFC) require firms to maintain effective surveillance of communications, in line with global expectations.

ASIC reaffirms that effective supervisory arrangements are crucial for managing conflicts of interest risk, including harms from:

- **Inappropriate or unauthorised disclosure** of confidential or inside information.
- **Market abuse**, including insider trading and market manipulation.
- **Bribery, fraud or other behaviour** that may be prohibited under law or a market intermediary's internal policies.



Regulators around the globe are making it clear they will not tolerate blind spots in eComms surveillance and archiving requirements. Firms need to ensure all business-related conversations, especially through established and emerging digital channels, are logged, monitored, and stored in compliance with the relevant regulatory standards.

By adopting proactive monitoring and proven RegTech solutions, firms can not only meet today's obligations but also position themselves to withstand the scrutiny of developing regulations.

MCO delivers streamlined solutions for monitoring and flagging risky communications and archiving cross-channel messages in compliance with global regulatory requirements. **eComms Review** and **eComms Keep** modules conduct intelligent surveillance and securely retain communications from Email, Zoom, Bloomberg, Reuters, ICE Chat, Skype, WhatsApp, Signal, SMS, LinkedIn, Teams and other channels, satisfying regulators' record-keeping rules and enabling more efficient investigations.

Managing Trade Surveillance Complexities

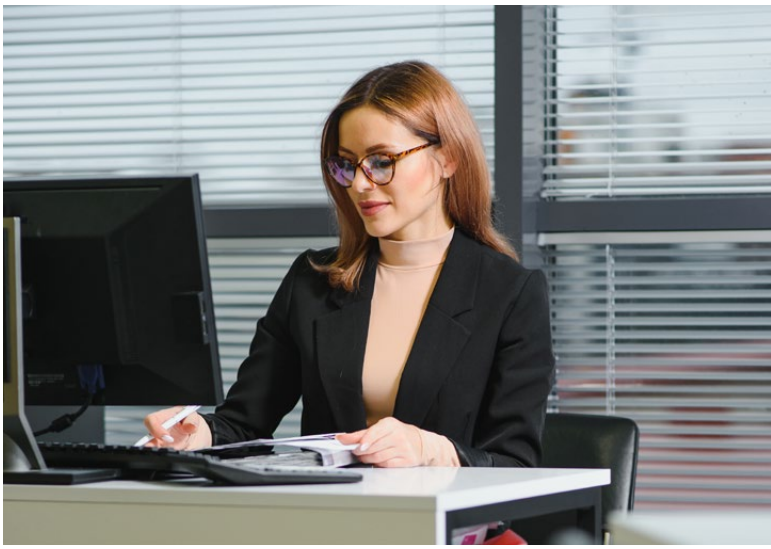
Trade surveillance in financial firms involves capturing transactional data and analysing it to identify potential market abuse and unethical or illegal trade practices. It is an essential practice in reducing the risk of market manipulation, fraud, money laundering, insider trading, and unsuitable investments.

While trade surveillance is a regulatory requirement, execution is becoming increasingly complex. Firms must capture and analyse trading activity regardless of employee location, with consistent controls across offices, branches and remote settings. Voice and electronic communications data are also integral to detecting suspicious patterns. The volume and variety of these data points continue to grow as interactions occur across multiple devices, channels and applications, requiring effective surveillance rules, storage, and reporting that can continue to scale.

When implementing or reviewing your trade surveillance setup, it's vital to check the following areas:

Scope

- Whether your trade surveillance program should include personal trading activity.
- The regulatory jurisdiction under which trades are occurring.



Monitoring

- Experienced staff with clear reporting lines that do not suggest any conflicts of interest.
- Monitor the status of any outstanding items and follow-up actions required.

Reporting

- Have adequate record-keeping processes in place to provide maintenance of surveillance records and documentation.
- Ensure proper storage of all data, including voice and eComms, for fast reporting to be made available if further investigation is needed or if requests from regulators are received.
- Make periodic reports with surveillance metrics available for senior management to review.

Analysis

- Analyse trade data in conjunction with voice and eComms data to help detect suspicious patterns and behaviours.
- Define your internal processes around when the analysis of suspicious trading activities should be escalated and the actions that should be taken.
- Review and analyse the quality and accuracy of alerts, closures, and escalations.

Automation

- Your surveillance process should be automated to help compliance officers analyse and identify potential issues data most effectively. Don't leave breaches falling through the cracks due to manual processes.
- Make sure automated alert processes match your criteria and assessment for flagging potential issues, your escalation policies, and the closure of alerts and escalations.

Proper surveillance enables firms to take proactive measures that identify and prevent market abuse and unethical or illegal trade practices. The right compliance management platform can take the complexity out of detecting, reporting, and taking action on potential issues.

Solutions such as MCO's Trade Surveillance module can help your firm monitor, report, analyse, and take action on wrongdoing without exhausting the time and attention of your compliance department. MCO's automated solution includes an extensive rules engine, customisable alerts and workflows, insider list and MNPI management, and much more.

Learn more about MCO's Trade Surveillance module

When Personal Trading Becomes Insider Trading

Conflicts of interest arise in personal trading (also known as personal account dealing) when securities transactions are made for an individual's direct or indirect benefit by leveraging an unfair advantage.

Personal trading crosses the line into insider trading when an individual trades, recommends, or causes trading while in possession of MNPI (including shares, options, bonds, and other financial products) and in breach of a duty of trust, confidence, or confidentiality. The information must be specific, non-public, and reasonably likely for a typical investor to view that data as influential in their investment decisions.

There are a range of circumstances in which the use of confidential information that is unavailable to the public can become instances of insider trading, including:

Tipping and Downstream Trading

Trading after receiving a tip, where there is a benefit gained of cash, quid pro quo, career advantage, or even an intention to gift trading profits to a friend or relative, or when sharing MNPI with another person who then trades for personal or shared benefits.

Shadow Trading

Using MNPI about one company to trade in the securities of another issuer, or a related instrument, that is likely to be affected by the same information. The trade exploits a foreseeable "spillover" effect rather than the issuer that is the direct subject of the MNPI.

Front-Running

Using knowledge of impending client transactions, block trades, buy-backs, or capital raisings to trade ahead for personal benefit.

Research and Wall-Crossing Breaches

Trading after receiving draft research, changes to recommendations, or wall-crossed deal details before public release.

Misuse of Confidential Company Information

Trading based on unreleased earnings, guidance changes, product launches, credit-rating actions, litigation outcomes, or M&A activity.

Trading Through Proxies

Using family, friends, trusts, and offshore or managed accounts in an attempt to conceal activity tied to the possession of MNPI.

The Impacts of Market Manipulation

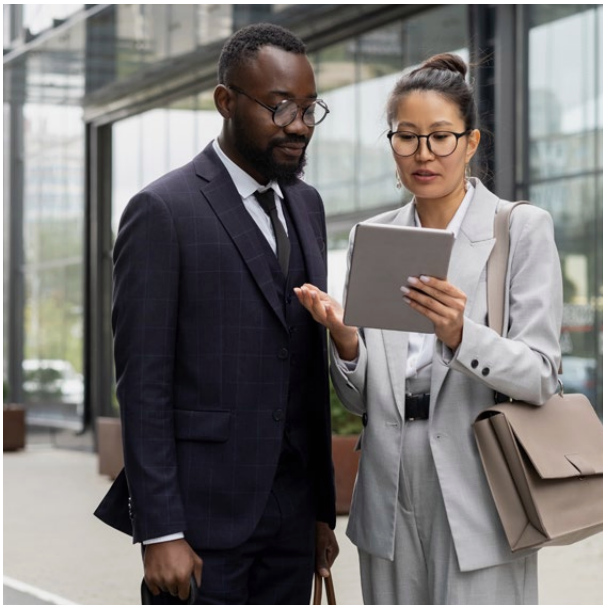
The wider-reaching effects of insider trading on economic markets are even more sizable. Financial markets rely heavily on liquidity which makes it easy to trade securities without affecting price. When markets are manipulated, liquidity is impacted, and investor returns are compromised.

Additionally, consumer confidence in financial markets can be severely damaged. As insider trading activity is uncovered, consumers can perceive markets to be “rigged” and their investment opportunities to be diminished.

The OECD reports that public investor ownership of the global stock market capitalisation sits at around 11 %[6].

When investor confidence is hurt, it can substantially impact overall economic growth.

Shadow Trading: Extending the Scope of Insider Trading



A recent case brought forward by the US SEC reaffirms that insider trading risk extends beyond the issuer that is the subject of MNPI. In the case, a federal court in California has upheld a jury verdict and civil penalty where an employee, holding confidential deal information about one company, bought options in a different listed company operating in a closely related market.

The court accepted that the information was material to the security actually traded because industry "spillover" effects were reasonably foreseeable. It also found a breach of duty grounded in confidentiality obligations and the firm's insider-trading policy, which banned trading in other public companies on the basis of inside information obtained through employment. The verdict, which saw the defendant liable for violating securities laws, could embolden the SEC to pursue more claims of "shadow trading".

The decision is a clear signal that trading in peer or related securities while in possession of MNPI can create a conflict of interest that meets the definitions of insider trading. It also suggests that public companies may begin implementing more restrictive securities trading policies for employees to account for "shadow trading" risks.

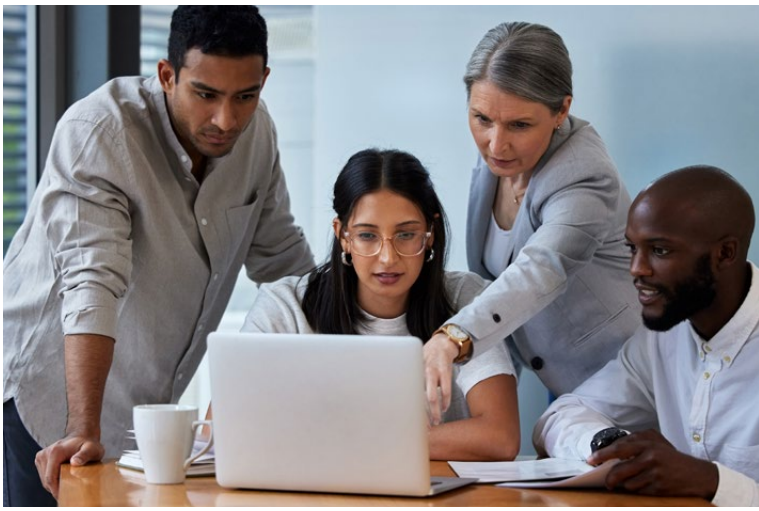
Financial firms would be wise to keep ahead of evolving regulations and implement personal trading policies that explicitly cover trading in peers, suppliers, customers and sector indices. Firms may also want to adjust pre-clearance processes to test for correlation risk, rather than issuer-specific restrictions alone. Additionally, training and attestations should reinforce these boundaries and the requirement to disclose MNPI access promptly.

Minimising the Risk of Insider Trading

While not all personal trades are likely to result in cases of insider trading, proactive monitoring and management of personal trading activity are critical. See the following steps that every compliance department can take to reduce risk.

Implement robust policies and procedures:

- Clearly define acceptable and unacceptable behaviour when employees engage in personal trades.
- Outline how monitoring and reporting will happen on all personal trading activity.
- Specify how you will regulate the trading of securities by key management personnel, directors, executives, and anyone with access to MNPI.



Deliver training across your organisation:

- Communicate your policies with training mechanisms that let employees raise questions or create dialogues about ethical and compliant trading behaviours.
- Help employees understand the consequences of insider trading and how they can avoid conflicts of interest.
- Provide guidelines for reporting potential conflicts of interest and communicate policies for the confidentiality of "whistleblowers" identities.

Define and communicate blackout periods:

- Make sure everyone understands blackout periods and trading windows to prevent anyone in possession of MNPI making personal trades during times when that information is likely to create unfair gains from transactions.
- Remind staff that blackout periods are commonly observed before the release of publicly-traded company earnings reports, M&As (mergers and acquisitions), or strategic investment activities.
- Ensure all employees know when blackout periods and trading windows will commence and end.

Record and maintain insider lists:

- Make it mandatory within your personal trading policy for employees to disclose any conflicts of interest (such as possession of MNPI) and inform compliance teams when changes happen.
- Maintain a list of those with MNPI, including employees, contractors, advisors, accountants, and other resources who may come in contact with sensitive information during business dealings.
- Have accurate data about contact details, why these people are on the insider list, and dated additions and changes.

Have a pre-clearance process in place:

- A documented pre-clearance process enables employees to request permission to make personal trade transactions of the organisation's securities, and ensures that personal trades avoid conflicts of interest.
- The process also allows the relevant organisational authority, e.g. chief compliance officer, chief financial officer, or other senior officers, to properly evaluate whether the personal trading activity should be approved or denied.

Monitor personal trading activity:

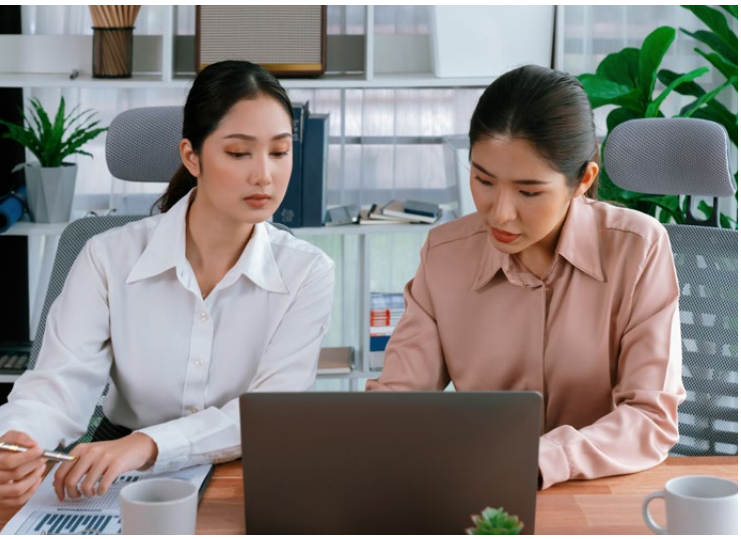
- Make it part of your procedures to monitor trading activity continually.
- Pay close attention to irregularities in employee trading patterns, which can sometimes be an early indicator of insider trading activity.
- Follow up and review changes and irregularities, as they may uncover broader patterns occurring over extended periods.

By factoring insider trading risk factors into policies, pre-clearance, surveillance rules, insider-list governance, and training, firms can strengthen deterrence. Importantly, they can also provide evidence to regulatory bodies of risk mitigation, identification, and escalation of potential insider dealing activity.

Regulatory Technology (RegTech) solutions are enabling firms to automate processes in line with policies and evolving regulations. Compliance resources can save significant time while ensuring full audit trails of all requests, approvals, and denials by using a compliance management software solution instead of outdated manual processes.

MCO's Personal Trade Manager enables policy-driven pre-clearance, configurable rules, restricted list checks, and exception reporting for employee trading, including crypto assets, to comply with personal account dealing and conflict-of-interest rules. Additionally, PTM's workflows record approvals, denials and rationales, creating evidence that firms have assessed and mitigated insider trading risk, in line with regulatory expectations.

Learn more about MCO's Personal Trade Manager



Monitoring and Managing MNPI

Access to MNPI is often at the heart of market-abuse risks. Employees can sometimes be exposed to this sensitive information from board papers, draft research, earnings and guidance, deal pipelines, regulatory decisions, litigation, and market soundings. For firms to prevent MNPI misuse, they must identify where it is generated or received, restrict access on a need-to-know basis, and record when and how individuals are wall-crossed.

Clear policies are also key to helping employees know the firm's expectations around MNPI. They should clearly define MNPI, explain when trading is prohibited, and set rules for disclosures, pre-clearance, and escalations. Training and attestations reinforce these standards and help staff recognise situations that can create MNPI, including informal conversations with clients, advisers, and counterparties.

Effective oversight of MNPI relies on traceability. Compliance teams need fast visibility of who had access, when access changed, and what controls were in place at each stage. Technology should also support the firm through consistent capture of MNPI access events, automated linkage to pre-clearance and surveillance rules, and rapid production of records for regulators. Firms that treat MNPI management as an end-to-end control framework are better placed to deter misconduct, detect issues early, and demonstrate compliance when under regulatory scrutiny.

Understanding Insider Lists

A list of people who have access to MNPI is called an "insider list". These lists can include employees and anyone outside the organisation who has access to insider information, such as contractors, advisors, accountants, and other resources who may come in contact with MNPI during business dealings.

Your records should maintain accurate information about these people's contact details, why they are on the insider list, and dated additions and changes to the list.

It is also crucial to record when people are removed from insider lists to identify when they stopped being in possession of MNPI. Insider lists are vital when responding to requests for information from regulatory bodies during market surveillance activities.

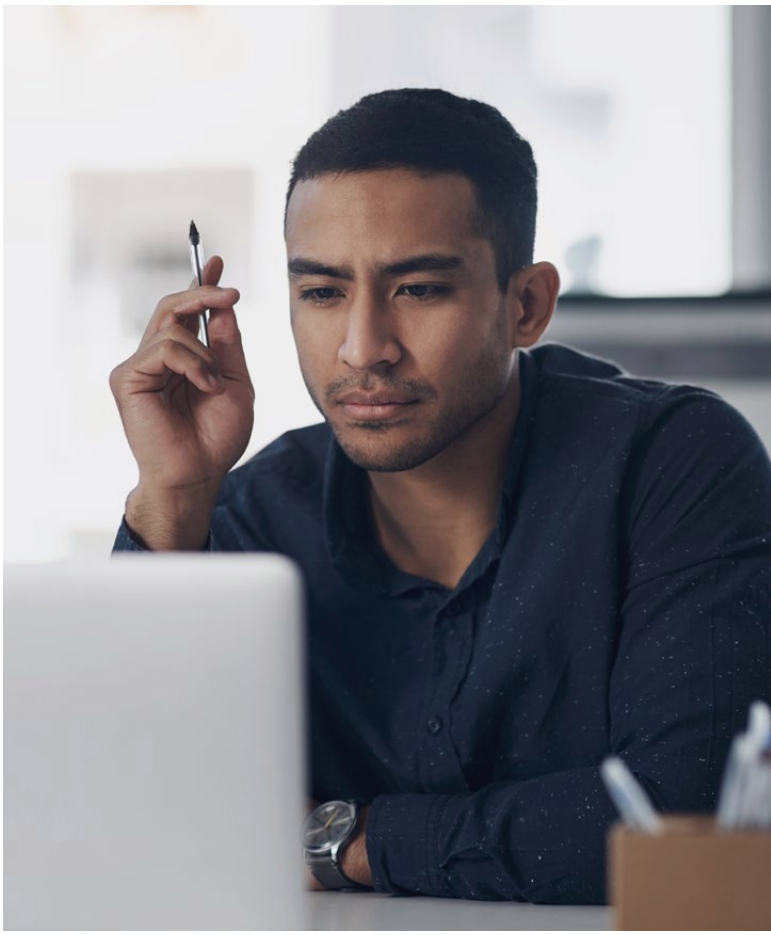
Building Efficiency into Insider List and MNPI Management

Insider lists and tracking of employees with MNPI can become complex and labour-intensive to manage through spreadsheets and disconnected systems. So when further investigation is needed or when regulatory bodies request information, systems that automate the capture, maintenance, and reporting of your data offer considerable benefits to compliance teams.

When implementing or reviewing the appropriate compliance management solution for managing insider lists and MNPI, ensure that it will:

- **Capture data** including MNPI summary information, details of who had access to MNPI and when, and dated histories of when access occurred, changed, or was relinquished.
- Allow for separate **'event insider' lists** to capture details of people given temporary access to information based on events, such as deals, corporate events, and publications of financial statements or profit warnings.
- Allow for separate **'permanent insider' lists** to track anyone with access to inside information at all times.
- Support a **review process** for compliance teams to formally validate the MNPI being monitored and reported.
- Quickly produce **accurate reporting** as required by the regulatory bodies of your region(s).
- **Centralise and streamline** information. With a centralised solution that includes insider list and MNPI management as part of a larger compliance suite, you'll minimise the number of systems compliance personnel need to learn and navigate daily, further boosting productivity.

Regulatory Technology (RegTech) solutions such as MyComplianceOffice can record MNPI access events, link insider, watch and restricted lists to policy-driven pre-clearance and surveillance rules, and provide auditable reports and case files to evidence controls and respond quickly to regulatory requests.



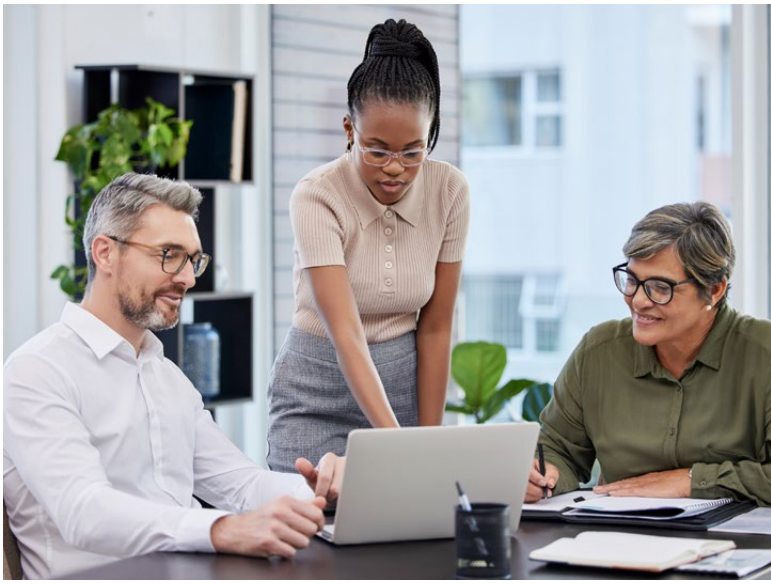
Lessons from Regulators on Managing Conflicts of Interest

Australian regulator ASIC recently announced proposed reforms to its guidance on managing conflicts of interest, marking the most substantial update to Regulatory Guide 181 (RG 181) since 2004. The new draft guidance outlines the regulator's expectations of FIs in identifying, assessing and managing conflicts across all areas of financial services businesses. It introduces a proportionate legal framework to ensure firms implement arrangements that are robust, effective, and tailored to the specific risks of their firm.

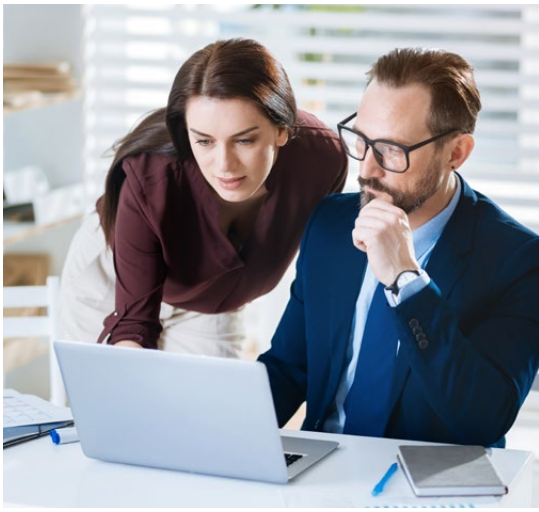
ASIC Commissioner Kate O'Rourke explains, "Conflicts of interest are more than mere moral dilemmas. They can undermine trust, integrity, and performance, causing serious harm to consumers, investors, and overall market confidence."

To ensure compliance, ASIC proposes a four-step framework for licensees.

1. **Identify** conflict based on "general risk and materiality posed by a conflict or class of conflicts" and the risks posed by a conflict of interest or class of conflicts.
2. **Assess** its risk and materiality, including undertaking a "risk assessment of a conflict of interest or class of conflicts and evaluating what an appropriate response would be".
3. **Respond** appropriately to effectively manage a conflict of interest, including having "arrangements to evaluate and monitor the effectiveness of your specific response and rectifying or providing remedial action if the response is not effective".
4. **Implement**, monitor, maintain, and review arrangements to ensure they remain robust and effective, including senior management and (where appropriate) board endorsement, staff and relevant party training, compliance monitoring systems, and accountability and disciplinary measures.



Technology's Role in Identifying and Addressing Conflicts of Interest



Every financial firm, regardless of size or strategy, deserves the tools to confidently operate in a compliant manner and protect itself from financial and reputational harm. Technology plays a vital role in helping firms uphold regulatory expectations and reduce risk from conflicts of interest.

MyComplianceOffice exists to help financial institutions:

- **Track and manage** conflicts of interest.
- **Make it easy** for employees to declare conflicts and provide attestations.
- **Monitor** employee close personal relationships to identify potential conflicts of interest.
- Manage **ongoing learning** and licensing requirements to ensure employees are deemed "fit and proper" for the requirements of their roles.
- Monitor and identify **red flags** in personal trading activity.
- Proactively flag high-risk electronic **employee communications**.
- Maintain comprehensive archives of eComms data to comply with regulatory and **record-keeping requirements**.

Most importantly, MCO assists firms in the following ways:

- **Identify** conflicts by enabling Business Managers to record conflict risks for their business, monitor those risks on an ongoing basis, and link them to the appropriate controls through our Know Your Obligations – Compliance Risk Manager.
- **Assess** conflicts by conducting initial and ongoing risk assessments, including the controls it plans to put in place if it eventuates.
- **Respond** to conflicts identified by reviewing identified conflict alerts within our Know Your Transactions and Know Your Employee suites, creating once-off, or regular tasks to manage the control, control plans and case management.
- **Implement** appropriate controls, by documenting internal committee memberships, roles & responsibilities of senior leadership, certifications, records of training, fit & proper assessments within our Roles and Responsibilities module, and regular control test plans of any conflict risks at the Group or Business Unit levels.

MCO's integrated compliance management suite enables firms to identify conflicts of interest more efficiently across their organisation. MCO provides a consolidated platform for compliance teams to manage areas of potential conflict, including:

- Personal account dealing
- Trade surveillance
- MNPI disclosure
- Close personal relationships
- Attestations, registrations and licences
- Outside business activities
- Gifts, entertainment, and hospitality

References:

[1] https://www.sec.gov/newsroom/press-releases/2024-178

[2] https://www.hkma.gov.hk/eng/news-and-media/press-releases/2025/01/20250127-4/

[3] https://www.sec.gov/newsroom/press-releases/2024-186

[4] https://www.fca.org.uk/news/news-stories/2024-fines

[5] https://www.asic.gov.au/about-asic/asic-investigations-and-enforcement/asic-enforcement-outcomes/

[6] https://www.oecd.org/en/publications/oecd-corporate-governance-factbook_31d6ea0b-en.html

[7] https://www.staffingindustry.com/news/global-daily-news/almost-all-us-job-seekers-have-side-hustles-41-work-on-them-during-company-time

[8] https://www.fca.org.uk/publications/multi-firm-reviews/multi-firm-review-off-channel-communications

[9] https://www.asic.gov.au/regulatory-resources/markets/market-supervision/supervising-your-representatives-business-communications/