



# Closing the Gaps in Trade Compliance

**Connecting Personal Account Dealing,  
Insider Risk and Surveillance**

## Table of Contents

Regulatory Environment .....	3
Enforcement .....	4
Compliance Approach .....	5
The Compliance Data Gap .....	6
Management of Insider Information.....	6
Verification of Trading Activity .....	7
One Platform. Total Oversight. ....	8

Managing Personal Account Dealing (PAD), insider information, and trade surveillance across separate systems obscures risk, limiting a firm’s ability to identify and act on connections between access to sensitive data and employee trading activity.

**Managing Personal Account Dealing is a core component of meeting both internal policy obligations and regulatory requirements. However, when PAD oversight operates independently from insider risk management and firm-wide trade surveillance, critical context is lost—creating gaps in both compliance and risk detection.**

Employee personal trading raises a number of compliance and risk issues that firms must address, including the management of inside information, conflicts of interest, and the potential for market abuse. Effective oversight requires a holistic approach: supervision of employee trading must be integrated into the broader compliance and risk management framework. This includes not only monitoring trades but also ensuring the firm has the capacity to manage the flow of inside information, detect breaches, and identify other improper activity.

By linking PAD with insider risk and enterprise-wide trade surveillance, firms gain a unified view of potential exposures. This integrated approach strengthens detection, supports regulatory compliance, and provides a clear, auditable record of employee activity within the wider context of firm risk.

## Regulatory Environment

**Regulatory requirements are broad, requiring firms to manage personal account dealing in the wider context of insider information, conflicts of interest, and market abuse.**

While firms must adhere to regulatory requirements including **MiFID II** (Markets in Financial Instruments Directive II), the **UK Financial Conduct Authority's (FCA) COBS 11** and related local laws to have “adequate arrangements” to address Personal Account Dealing, a broader and more fundamental approach that includes managing the flow of insider information, conflicts of interest and market abuse is at the heart of successful employee personal trading management.

In Europe and the UK, market abuse is subject to the **Market Abuse Regulation**. Market

abuse covers insider dealing, the unlawful disclosure of inside information and market manipulation including front running. Anyone in a firm with access—or potential access—to inside or client confidential information must be covered by the firm’s overarching policy on the management of inside information. As a matter of course, the approach to employee personal account dealing should be interwoven into firm-wide management of inside and confidential information.



# Enforcement

Enforcement actions consistently demonstrate that failures in personal account dealing controls are rarely isolated—they often expose broader weaknesses in governance, surveillance, and insider risk management.

There are numerous recent examples of corporate and individual liability including:

- In June 2024, Sweden's **Finansinspektionen fined a stock exchange SEK 100 million** for deficiencies in its trading monitoring, which should have been designed to prevent, identify and report insider dealing. The exchange also, on two occasions, initiated trading in financial instruments in breach of the regulatory framework.
- In July 2024, the **Autorité des Marchés Financiers (AMF) fined an issuer €150,000 and sanctioned two of its former directors** for market manipulation through the dissemination of false or misleading information. One director received an additional fine of €210,000 for insider trading.
- In February 2025, the **Financial Conduct Authority (FCA) confiscated £586,711.01** from an individual convicted of insider dealing and sentenced to 22 months in prison. Critically, the confiscation order amounts to all of the individual's available assets.
- In July 2025, the AMF **fined eight individuals and two corporate entities a total of €1.89 million** for insider dealing and late disclosure of inside information, highlighting systemic failings in the management and dissemination of price-sensitive information.
- In July 2025, the FCA **fined a brokerage firm £1.09 million** for transaction reporting failures under MiFIR. Incorrect system configuration caused nearly 925,000 inaccurate reports — close to 100% of the firm's transactions — to go uncorrected for five years.
- In December 2025, the FCA **fined a retail financial institution £44.1 million** for inadequate anti-financial crime systems and controls, including failures in customer due diligence and transaction monitoring across its personal current account base.



Effective compliance is not defined by individual controls—it is defined by the strength of the compliance chain that connects them.

## Compliance Approach

**The Market Abuse Regulation sets out required outcomes, such as maintaining insider lists, but it does not prescribe exactly how firms should comply.**

While this gives firms flexibility in their approach, any method must be integrated into the broader suite of controls, policies, and procedures that not only manage the business but also provide clear evidence of compliance.

Today, every aspect of financial services is viewed through a lens of conduct risk and culture expectations. It is no longer sufficient for a firm to simply follow the rulebook. Regulators now expect firms—and their senior managers—to demonstrate that they have acted appropriately, followed sound processes, and consistently delivered good customer outcomes.

Effective management of employee personal trading activity is underpinned by a set of core controls. A key principle is that all employees—and relevant contractors, outsourcers, appointed representatives, and agents—should annually attest that they have read, understood, and agree to abide by the firm’s personal account dealing rules. This attestation creates a clear audit trail and removes any claim that employees were unaware of the requirements.

## Best Practice Controls Around Personal Account Dealing and Insider Risk

- Pre-clearance of personal trades
- Automated capture and reconciliation of trading activity
- Restricted and insider list management
- Employee attestations and policy acknowledgements
- Surveillance of employee and related-party trading

# The Compliance Data Gap

**While personal trading and insider risk controls can be individually effective, managing them in isolation can create inefficiencies and blind spots.**

A siloed approach leaves compliance data fragmented across multiple systems, including trading platforms, insider lists, and surveillance tools. Risk emerges in the gaps between these systems, where connections between information access and trading behavior are often not visible.

Effective compliance means viewing trading compliance as a continuum—one that treats the process as an interrelated chain of events: who had access to insider information, who has been trading, and whether those with access to insider information have traded and used that information for illegal gain.

Not all trading risk stems from deliberate misconduct. Accidental exposure to inside information presents a significant and often underestimated risk to both individuals and the firm.

## Management of Insider Information

**With inside information flowing across multiple channels and functions, firms must adopt a more structured and controlled approach to its management.**

Proactive management of inside information across a firm is at the core of effectively managing both personal account dealing and the risk of market abuse. And with information coming at employees at all different angles, it's a challenge that can't effectively be managed on a spreadsheet.

Firms must have clear line of sight into who has access to what information, when, and on what basis. This can represent a cultural shift for firms that have previously taken a more open and universal approach to information access across the organisation. Demonstrably effective management of inside information can enable better business practices—if firms have the data to minimize who needs to operate under restrictions, there is less need to wall off the entire organization.

# Verification of Trading Activity

**Firms need to go full circle with the oversight of personal account dealing.**

Preclearance of trades is an essential first step, but then the executed trade must be matched against the clearance given. This can involve reconciliation against either electronic or paper-copy contract notes, both of which will need a comprehensive audit trail to evidence compliance monitoring.

Any trading identified as occurring outside of the clearance given should be investigated. Where possible, the oversight should extend to cross-referencing the personal trading against that carried out by other employees, friends, family members, as well as the potential for shadow or pairs trading. And as a matter of course, the preclearance process must use up-to-date restricted lists as the basis for granting or denying permission to trade.

For the effective oversight of trading activity, firms must have embedded processes that effectively identify insider trading and market abuse, detect suspicious trading patterns and policy violations, and can evidence to regulators that the firm has fair, transparent and compliant trading practices.

## Expanding Insider Risk Oversight to Digital Assets

As employee trading expands into crypto and other digital assets, firms must ensure that existing Personal Account Dealing and insider risk frameworks evolve to capture these activities with the same level of rigor as traditional markets.

Integrating trading activity across traditional and digital asset classes into a unified compliance platform ensures firms maintain full visibility, strengthen controls, and mitigate emerging risks in line with regulatory expectations.

# One Platform. Total Oversight.

**A unified compliance platform enables firms to connect insider information, employee trading activity, and firm-wide surveillance—delivering a complete, auditable view of risk.**


MCO empowers firms to reduce regulatory risk by monitoring and managing all trading compliance functions through a unified solution. With MyComplianceOffice, firms can eliminate silos and inefficiencies by bringing inside information management, personal trading surveillance, and trade surveillance together on a single platform—enabling firms to:

- Pinpoint who has access to inside information and when it was received
- Detect potential misuse of information by analysing employee trading activity and the trading activity of related persons
- Identify potential abuse by monitoring trading activity across the firm

Critically, managing these capabilities on one platform improves efficiency, enhances accuracy, and drives standardisation across the firm's compliance program, while providing a defensible audit trail for regulators and the board.

With 1,500+ clients across more than 125 countries, MCO supports firms in meeting complex regulatory obligations while delivering more effective and streamlined oversight of trading activities.

For more details on how MCO can help visit [MyComplianceOffice.com](https://mycomplianceoffice.com) or contact [advance@mycomplianceoffice.com](mailto:advance@mycomplianceoffice.com).



**MCO (MyComplianceOffice) provides compliance management software that enables companies around the world to reduce their risk of misconduct and effectively oversee regulatory obligations.**

Our powerful platform lets compliance professionals demonstrate they are proactively managing the regulated activities of the company, employees and third-party vendors and provide evidence of regulatory compliance. Available as a unified suite or à la carte, our easy-to-use and extensible SaaS-based solutions get firms up and running quickly and cost-efficiently.