

The **MNPI Compliance** Handbook

Introduction: How we ended up in the current state of play

In recent years, there has been an increase in the number of cases where regulators have cracked down on firms and individuals for insider trading and the improper use of material, nonpublic information (MNPI). For example in FY 2022, the SEC brought [43 insider trading cases against 93 individuals](#) compared to [28 cases against 47 individuals in 2021](#).



This was one of the factors that drove the SEC to announce \$6.439 billion in penalties (the most on record), up from \$3.852 billion in FY 2021. In the UK, the FCA brought 72 insider dealing cases and received [3,367 insider dealing Suspicious Transaction and Order Reports \(STORs\) in 2022](#). And in the EU, [ESMA received 2,566 insider dealing STORs](#).

While bad actors will always exist, monitoring who has access to MNPI doesn't need to be a challenging process. Nor, does it need to be managed via the ['swivel chair' approach](#) – where Compliance professionals dig through multiple applications, emails, excel sheets, and other siloed materials across the business to create one source of truth for identifying potential risks before they turn into larger problems. This swivel chair approach to MNPI can be traced back to the implementation of the [Insider Trading & Securities Fraud Enforcement Act of 1988](#) (ITSFEA) in the US. And while ITSFEA set the tone for what we expected from firms and required broker-dealers in developing the adequate policies and procedures to prevent and detect the misuse of MNPI, it is a heavily manual process, is prone to human error, and lacks the agility needed to manage the data as information changes.

Further efforts to complement the ITSFEA regulation were advanced by the [SEC in 1990](#), when it released broker-dealer policies and procedures designed to segment the flow and prevent the misuse of material, nonpublic information to investigate the adequacy of federal securities laws surrounding insider trading. This report came out of a comprehensive review of broker-dealer policies and procedures and included an assessment of how well self-regulatory organizations (SROs) oversaw member firms' information barrier activity. A primary finding of this report was that no two compliance infrastructures to control the flow of MNPI were alike and the SEC recommended that firms memorialize in greater detail their procedures, and similarly improve the documentation, communication, and recordkeeping associated with information barrier activities.

In 1991, the National Association of Securities Dealers (now FINRA), the New York Stock Exchange, and the Securities Industry Association (now SIFMA) released a [joint memo](#) that laid out the minimum elements of adequate information barrier policies and procedures pursuant to ITSFEA requirements.

Based on this guidance firms began to memorialize policies and procedures, surveil employee and proprietary trading, supervise interdepartmental communications, and conduct training. By 1992 the bulge-bracket firms officially started to develop their own controls to effectively capture the flow of MNPI, without anyone else ever having done it before.

Since then, regulations have evolved with more coming into play to further prevent the misuse of MNPI.

For instance, the EU adopted the [Market Abuse Regulation \(MAR\)](#) in 2016 aimed at increasing market integrity and investor protection, including use of inside information, and prohibiting insider dealing. Similarly, Canada, Australia, Hong Kong, Japan, Singapore, and Malaysia all have specific rules that address insider trading and the misuse of MNPI.

Recently, the SEC's pace of new and proposed rules and investigations have been moving at record velocity, including [amendments to Rule 10b5-1](#), [amendments to the Investment Adviser Act 206\(4\)-7 to document annual reviews](#), [adoption of Rule 15fh-4\(c\) to prohibit undue influence over the CCO's](#), and eccentric focus on crypto continues to put unimaginable pressure on compliance officers. Not to mention the SEC's willingness to pursue novel cases like [shadow trading](#), which involved using MNPI of one company to trade – not in the stock of that company, but in the stock of an entirely different (competitor) company. Or the SEC's recent actions against crypto firms and exchanges like [Binance](#), [Coinbase](#), [Ripple](#), [Titan](#) and [Impact Theory](#).

When one takes into consideration the diversity of capital markets, rising global regulation and employees no longer working completely in traditional office spaces, one can see how the strain on Compliance is even greater today when trying to manage MNPI.

This is where modern, automated technology comes in, designed from the ground up specifically for capturing and monitoring the flow of MNPI. Technology that can help streamline and automate MNPI compliance processes, with all critical information and activities executed, monitored, and logged through one source of truth. Technology that allows employees to self-report MNPI and ensure Compliance captures all relevant, required information from the start, eliminating the back and forth and mile-long email chains with employees – making risk mitigation that much easier.

This guide will take you step-by-step through the development and implementation of robust MNPI processes. It will enable you to get the most out of the resources at your disposal, while ensuring you have an organized track record of all your people who have access to MNPI so that you can more easily monitor for risk and comply with confidence.



TABLE OF CONTENTS

SECTION 1: Do Your MNPI Processes Need a Refresh?

SECTION 2: Determining Scope and Mandate

SECTION 3: Building MNPI Information Barriers

SECTION 4: Optimizing Your MNPI Processes

SECTION 5: The Future of MNPI



Do Your MNPI Processes Need a Refresh?

That depends on a whole host of factors, from the type of activity and MNPI you're dealing with to what happens when someone does something they shouldn't have.

Type of activity, breadth of activity, and MNPI

The truth is, there aren't explicit rules or job descriptions that speak to how firms should track and manage MNPI. Global regulations simply state that firms need to have 'adequate policies and procedures in place to prevent and detect insider trading'. It's up to firms to assess the markets, products, and services they offer, determine which generate MNPI and which don't, and then develop the processes to monitor and control its flow.

Size has something to do with it, but not everything. It also comes down to breadth of activity, the amount of MNPI in play, and the kind of business activities the firm engages in.

- Does the firm conduct private equity transactions?
- Does it assist with M&A advisory or acquisition financing?
- Does the firm offer equity or fixed-income research to support sales and trading efforts?
- Does the firm offer wealth or asset management services?
- Is the firm engaging in a market sounding event, such as the underwriting of securities?

The list goes on. But it's when these types of business activities and resulting regulatory challenges start to appear—where existing controls need to be enhanced to manage the risk—that manual processes quickly become inefficient, and a real need emerges for an automated MNPI solution.

Often, it's Compliance who identify the need for compliance support, but other times it's the Business saying: 'We're doing M&A, trading, sales, research, or asset management. There's a lot of MNPI, and we need better controls to monitor the flow.' They'll demand the firm have proper processes, people, and technology in place. Individuals that understand the firm needs to avoid regulatory and reputation risk to succeed. One knows they are operating in a good environment when the business is demanding that Compliance up its game.

Someone misappropriates information

Sometimes, an unfortunate event occurs that becomes the impetus for automation or formalization of stronger MNPI processes. Someone does something they shouldn't have, and a regulator issues a fine or a cease-and-desist order.

Perhaps an employee trades on inside information by accessing files containing MNPI, or someone fails to report a Watch List item where the firm has received MNPI. All these instances lead to regulatory and/or policy violations. In these cases, regulators may also require firms to retain an independent consultant to address deficient areas.

Firms should also recognize that there are real distinctions between regulatory violations and policy violations. If someone doesn't pre-approve a trade, as long as they're not trading on inside information, it's a policy violation. Not to downplay policy violations but focusing on the risk spectrum there's a big difference between policy violations and regulatory violations. Firms simply can't mess around with regulatory violations. No one should trade on inside information, fail to monitor research, or fail to report Watch or Restricted List items. These are all potential regulatory violations.

And if one thinks that perhaps regulations are one area that's black and white, where the lines are clear-cut and easy to follow, you're mistaken. Like with most things regulatory when it comes to insider trading, market manipulation, and fraud, you're often told what you're supposed to do, but not how to do it. That's up to each firm to figure out. With employee trading, the rules are clear. With sales, there are clear rules surrounding suitability and customer onboarding. But when it comes to information barriers, manipulation, insider trading, and MNPI, firms must turn to case law, rule interpretations, and industry precedent to determine the best course. It's good to have people on staff with industry contacts—colleagues they can reach out to—and the firm needs connections to consultants and legal counsel to tap into critical insights and best practices.



2

Determining Scope and Mandate

If you think your firm needs a better way of managing and tracking MNPI, then the time to re-imagine the concept on a practical level is now - how it should look and how to think about making the case for it.

Your first step is to assess the business. At this point, you know enough about it to know you need better processes. But now you must think about the specifics—precisely what activities the firm is already engaged in or will be engaged in—to determine scope and coverage. In short, you want to have a conversation with the business.

Assess who has access to MNPI

The starting point is to assess what businesses and employees have access to MNPI and should therefore be monitored more closely. A lot of critical information zips around a firm at any given time, and MNPI can originate from the private as well as the public side of the information barrier. But no matter where it comes from, unaccounted for MNPI and breaches of the information barrier can put the business and its reputation at risk. At this point, you'll need to undertake a risk-assessment that will position the firm to be able to properly develop and implement policies and procedures.

This risk assessment should include:

- ☐ All legal entities.
- ☐ The rules, regulations, and market conventions applicable to each business.
- ☐ Industry best practices for protecting client and customer information.



Potential steps in the risk assessment may include:

- ☐ Conducting interviews to assess each business unit.
- ☐ Assessing legal entities and regulatory requirements.
- ☐ Assessing the physical location of employees in all facilities.
- ☐ Taking inventory of the types of products offered by each business unit.
- ☐ Taking inventory of the types of MNPI obtained and generated by business units.
- ☐ Identifying types of material produced by business units assessing how the businesses interact with each other.
- ☐ Identifying the back-office support the front-office businesses rely upon.
- ☐ Assessing the licensing and supervisory universe, including who's licensed vs. who's required to be.



Here are specifics to think about as you begin to outline scope and mandate for your MNPI processes:

- > What happens when there's too much information and too many employees to adequately monitor with the controls, policies, and procedures you have in place? What's at risk? How much risk is the firm willing to take to entertain?
- > At some point your employees will become aware of MNPI. What are you going to do when this occurs? What are the controls that will be put in place? All firms must develop policies, procedures, and training to deal with instances when employees become aware of MNPI and will need to be maintained and regularly reviewed.
- > Smaller firms reach an inflection point where they have too many employees, too much information in motion, and not enough Compliance resources or automation. Are you at that point? If not, can you define what that inflection point would look like so you can be prepared?
- > Ultimately, Compliance leadership will need to balance staffing with automation. This may mean adding internal headcount, utilizing outsourcing, or offshoring, and developing or purchasing automation tools. Make sure you have a line item in your scope for the cost of such people and tech.

Here are some things to think about as you seek buy-in for a tool to help manage and monitor MNPI:

- > If leadership doesn't understand or doesn't have experience dealing with MNPI, then Compliance management will need to educate leadership of the regulatory risks and reputational challenges. Be prepared to educate, and to share real life examples of firms who may have allowed risk to go unmonitored for too long.
- > Make sure leadership understands the current state of affairs—inefficiencies or overloads the firm is facing that might indicate change is needed. Do you have more employees than ever at the firm? Do you feel Compliance is understaffed in terms of managing all the risk and manual processes you face? Take this evidence to firm leadership and back it up with tangible data.
- > If people haven't come from more established firms—where they understand what is required and expected—employees are likely to complain about MNPI rigorous processes. While it's an overused phrase, tone from the top is important and can help curb complaints as the rest of the firm sees the level of support coming from leadership.
- > The tone from the top helps to build a [culture of compliance](#) and demonstrates to the rest of the firm that the processes Compliance is putting in place are critical to protecting both the firm and its employees. Without that tone from the top, it will be much harder to convince employees to adhere to the new MNPI policies and processes.
- > Establishing the appropriate culture is key. The message should come from senior management first and foremost, but middle management also has a responsibility to set the tone for relationship managers, bankers, portfolio managers, traders, sales, research, and support personnel.
- > Training is critical at every level of the organization so everyone understands the important role Compliance plays and why the oversight this department establishes is necessary for protecting against MNPI risks.

3

Building MNPI Information Barriers

After you've determined the scope and mandate of your MNPI processes, the next step is to ensure you establish the appropriate barriers, policies, procedures, controls, and training to avoid information leakage and mitigate MNPI risk.

Information Barriers, Policies, Procedures, Controls, and Training

Clearly established information barriers help physically and electronically separate employees that deal with MNPI. This requires firms to define and assign public-side, private-side, and above-the-wall personnel, including committee personnel. Operations and support-side personnel—including those in Compliance, Legal, Operations, Finance, Information Technology, Credit, and Risk Management—must also be considered in this assignment process. Useful tools firms should consider leveraging include human resource applications (e.g., Workday) which contain organizational hierarchies and structures. Compliance should determine if there is a way to plug into these HR systems and assign designations to employees. HR systems may also be helpful when assigning and tracking personnel for deal-team purposes.

When designing firm information barriers, it's helpful to leverage an inventory of MNPI to help inform policies, procedures, and controls. By methodically reviewing the types of activities and information the firm has, Compliance will be in a better position to create the appropriate infrastructure to support the businesses across legal entities, affiliates, and subsidiaries. This process will also be helpful in mapping out how information flows through the organization, which is important in identifying potential conflict areas. Out of this, firms may wish to create process maps or flow charts to visualize the flow of MNPI. These designation and assignment processes can also help identify any third parties, advisors, consultants, or temporary employees who need to be considered part of the new and improved MNPI processes.

Information Barrier

Public-Side Employees

- Sales & Trading
- Research
- Portfolio Management
- Wealth Advisory
- Asset Management
- Rates
- IT
- Operations
- Other Support

Above-The-Wall Employees

- Executive Management
- Senior Management
- Compliance
- Legal
- Credit

Private-Side Employees

- Corporate & Commercial Banking
- Capital Markets
- Private Equity
- Leveraged Finance
- Specialty Finance
- Financial Sponsors Coverage
- Project Finance
- Credit Solutions
- Loan Syndication
- Loan Syndication
- Private Equity



Managing The Flow And Sealing The Gaps

Action Items + Workbook

Conflicts Considerations

An important part of controlling the flow of MNPI is establishing a process to identify and manage conflicts. Firms should think about conflicts in four ways:

1. **Firm versus client**
2. **Client versus client**
3. **Employee versus client**
4. **Remote employees versus onsite**

Firms are most successful when they assemble cross-functional representatives from Corporate and Investment banking, Capital Markets, Private Equity, Asset Management, Compliance, Legal, and other risk-support functions to identify, discuss, and review:

- ☐ Potential areas of conflict.
- ☐ Where conflict-resolution gaps currently exist.
- ☐ The current business selection and conflicts-of-interest process in the relationship, pitch, origination, and approval process.
- ☐ The policy, process, and team tasked with researching potential conflicts, escalating, resolving, and documenting opportunities and engagements.
- ☐ Legal documents—including NDAs and engagement, commitment, and underwriting letters—which clarify scope of services provided and the ability to perform additional roles.
- ☐ Disclosures and consent, as regards notifying clients of existing or potential conflicts of interest.
- ☐ Fairness opinions regarding material relationships between the investment bank and involved firms (FINRA Rule 5150).
- ☐ Standards for frequent areas of conflict, i.e., the requirements firms adhere to when providing services like acquisition financing, fairness opinions, staple financing, research, and underwritings.

Watch & Restricted List Considerations

The primary tools firms should rely on to manage the flow of MNPI are Watch and Restricted Lists. One of the biggest challenges Compliance teams face is the timely collection of information to determine if a situation should be added to the Watch or Restricted List. Once that determination is made, keeping track of the opportunity to determine the next step—updating the Watch List notes, updating the project team, moving it to the Restricted List, or removing it from one of the lists all together—is of critical importance.

While there are tools that can make a compliance officer's job easier, what teams really need are employees who understand the firm's processes and risks and will promptly inform Compliance when a "trigger" occurs. It's up to each firm to determine when a trigger occurs.

> **For bankers**

It may be when a firm is likely to be engaged for a deal or a target portfolio company.

> **For Trading and Sales**

It may be when they learn material, nonpublic portfolio information from a buy-side firm.

> **For Portfolio Managers**

It may be when they learn of MNPI from a sell-side firm or issuer.

> **For Research**

It may be when they learn price-movement information from the CFO of a company they cover.

Whatever the trigger it ultimately comes down to proper training of covered employees to immediately notify Compliance of the event, so a determination may be made of what needs to be done. This is all part and parcel of the strict culture that needs to be ingrained in a firm if it wants to operate at the highest levels.

Above-The-Wall Versus Over-The-Wall Personnel

Inevitably, public and private-side employees must report to a manager. This group of senior managers is often referred to as “above-the-wall.” This should not be confused with “over-the-wall” employees. Above-the-wall personnel have a unique obligation to manage the firm while maintaining the sanctity of the information barrier. Significant consideration should occur prior to designating someone as above-the-wall. Once these managers have been identified, they must be tracked, trained, and monitored.

Over-the-wall situations generally occur when a public-side employee’s skills and knowledge are required to assist private-side bankers in executing a transaction. For example, Capital Markets bankers need to understand market demand or structural appetite from Sales or Trading to price a deal. These situations must also be closely controlled and monitored.

- > **Identify**
- > **Document**
- > **Train**
- > **Monitor**

These are the four processes to keep in mind when determining who is above-the-wall or over-the-wall, and how to manage both cohorts.

Write any additional notes here

Need-To-Know Standard

One of the most important principles in building an effective information barrier is creating a “need-to-know” culture. Simply put, a “need-to-know” exists if access to the information is vital to providing the client with the products or services it has requested. Examples of this situation include:

- ☒ Executing the client strategy or business purpose
- ☒ Managing the client relationship
- ☒ Complying with credit, legal, or compliance requirements
- ☒ Protecting firm exposure

One of the keys to a successful firm business model is creating and enforcing an effective information-barrier policy and sharing MNPI only on a need-to-know basis. As a general rule, firm employees with MNPI or confidential information must not share that information with those that aren’t on the client’s deal team, do not have a need to know, or are public-side individuals. Finally, creating a need-to-know culture is critical for managing firm conflicts and reputation risks. Implementing training will help cement the cultural shift at the firm.

Practical considerations include:

- ☐ Assessing supervisory reporting lines to determine if public-side employees are reporting to private-side supervisors. If these reporting lines exist, firms should determine if there are information barriers, MNPI, or need-to-know standards concerns.
- ☐ Assessing walls between origination and execution, portfolio management, secondary loan trading, and any portfolio management hedging activities.
- ☐ Working with the Business and IT to assess and assign system, application, and electronic folders access controls by client focus, job function, need-to-know, and organizational structure.
- ☐ Implementing CRM software controls, so only project teams and need-to-know users have access to client information.
- ☐ Plenty of need-to-know training.

Surveillance Considerations

Regulators require firms to prevent and detect potential misuse of MNPI. In addition, regulators are becoming more proficient with analyzing large data sets to bring fines and sanctions against firms. The ability to conduct surveillance is therefore critical, and should start with the basics: Conflict, Watch, and Restricted List surveillance of firm, customer, and employee activities. It is obvious firms must ensure they are capturing activities and comparing them with names on the Watch and Restricted Lists. But what do you do with this information? How do you record your analysis? What additional information should be added to support the surveillance?

And as we learned during the pandemic, the “line of sight” as we knew it as a compliance control, has changed and had to be reimagined. We’ve experienced the working world shift from traditional offices, to remote work, with a majority of firms now seemingly settling on a [hybrid work environment](#). This creates new challenges for firms to ensure all MNPI and related activities end up in the hands of Compliance.

Firms should develop a comprehensive and consistent employee and employee-related accounts policy that provides detailed requirements regarding permissible employee trading. Considerations may include:

- ☐ Requiring employees to maintain their accounts at a limited number of designated brokers to receive electronic feeds and eliminate paper statements.
- ☐ Requiring all employees and employee-related accounts to pre-approve all trades, not just trades in securities included on the Restricted List.
- ☐ Implementing business unit and conflict restrictions defined by employee type.
- ☐ Implementing a securities-holding period to discourage speculative trading, which could be an indication of potential manipulative activity. Holding periods are a common industry practice and typically range from 7 to 30 days.
- ☐ Imposing additional limitations on employee investments, e.g., no trading in options or futures.
- ☐ Requiring employees to attest they’ve disclosed all their employee and employee-related accounts in accordance with firm policies and procedures.



FREE DOWNLOAD

Certifications Checklist

Getting to the other side of the certification process can be challenging, our five-step approach Certification Checklist can help you prepare.

DOWNLOAD NOW

Pre-Trade (Preventative) Reviews & Approvals

Firms may wish to implement controls to restrict trading activities through order management system (OMS) configuration rules. For example, a firm may require additional approvals for trading Restricted List securities. Firms may also simplify and streamline employee personal trading using pre-clearance software that scans potential trades against: (1) Watch and Restricted Lists; (2) fund-trading activity; (3) holding periods; (4) blackout windows; and (5) de minimis thresholds. Finally, firms may facilitate testing of trading activity through automated electronic feeds from brokerage firms.

Post-Trade (Detective) Surveillance

Firms may wish to identify trading in securities where MNPI may be known. They may also use automated rules or statistical algorithms to identify patterns of trading activity that could indicate the use of MNPI based on multiple risk factors. These risk factors could include timing, capital-at-risk, or performance. Firms may also enhance their existing data sets—and by extension their ability to monitor insider trading—by incorporating third-party reference data such as market data and news feeds.

Electronic Communications (E-Comms) Surveillance

We all know that firms must monitor internal and external emails, instant messages (IMs) and chats. With the plethora of electronic communication applications available, identifying and capturing all vendors, services, and tools is a challenge. We also know that surveillance of internal and external electronic communications has become a standard part of compliance and supervision in the LIBOR and FTX scandals. Now the question is, what role should Compliance play in monitoring e-comms? One solution is incorporating Watch or Restricted List names into the monitoring lexicon. Firms obviously need to restrict and/or supervise e-comms between banking and research. Firms may also wish to monitor and/or restrict e-comms between banking and the rest of the public side—like Sales, Trading, Portfolio Managers and Wealth Management—and restrict project emails to non-deal team members or clients.

Firms should include testing communications to identify incoming or outgoing MNPI, customer communication patterns vs. sales and trading activity, and relationships of interest. Firms should include email, chats, Bloomberg, IM, and other web-based mail and social networking sites as used on firm networks. As firms mature, they should consider incorporating surveillance and analysis of telephone logs, calendar entries, and gifts-and-entertainment logs.

It goes without saying that surveillance controls should be adjusted over time to incorporate lessons learned and market changes.

Write any additional notes here

Other areas of concern and potential abuse firms should not ignore include:

- ☐ Loan trading
- ☐ Distress trading
- ☐ Over-the-wall activities
- ☐ Market-moving events and regulatory filings
- ☐ Front running, i.e., trading ahead of a client, research, M&A, and capital market events
- ☐ MNPI produced "outside the four walls" of the firm

Information Security & Employee Electronic Access

Do your information security protocols limit who can see client, project, and borrower specific information, especially for public companies? To bolster information barriers, firms should assess system controls—including pipelines, CRMs, confidential files, credit and loan portfolio files—to determine if access controls are sufficient.

Firms have the best results when Compliance works with first-line businesses and IT to assess and assign system access across the board by client focus, job function, need to know, and organizational structure.

Procedures should also be developed to limit project team folder access to only members of the project team, and controls developed to limit and monitor access and training on protecting client information. If unauthorized access is discovered, firms should investigate the situation and determine what actions should be taken.

Training & Reviews

After establishing comprehensive policies and procedures, firms must design compelling training programs that are more than just rote and one-size-fits-all. Firms should tailor training specific to the business unit and employee. Think of creating a bespoke training plan for each business and type of employee.

Insider Trading Training

Promote:

Overall awareness and understanding

Training element:

- Identify key terms related to insider trading.
- Identify rules and regulations governing insider trading, including institution-specific guidelines, responsibilities, obligations, and prohibitions.
- Train rigorously on information barriers, conflicts, and personal investment policy.

An understanding of what applies to each employee and why

- To illustrate real-life risks, use situations that your employees are likely to encounter.

An understanding of consequences of noncompliance

- Use actual enforcement cases to demonstrate consequences.
- Always involve senior management in delivering key messages.
- Use case law, news articles, real life examples, and frequent compliance bulletins to illustrate lessons learned.

An understanding of gray areas, and how to reach out when the employee has questions.

- Use scenario-based situations, based on client-specific examples.

4

Optimising Your MNPI Processes

Optimization requires automation, and technology is vital for preventing and detecting the misuse of MNPI and meeting global regulatory requirements. Here's what a good MNPI software management solution looks like:



Centralized, comprehensive Monitoring of MNPI

Policy violations (e.g., an employee failing to pre-clear a trade) are unwelcome occurrences. But regulatory violations (e.g., an employee trading on insider information; front running portfolio trades; trading in violation of [Regulation M](#) or [MAR](#); or the firm issuing research during a distribution when there is no safe harbor) are an altogether different story. A regulatory violation will likely involve a prolonged investigation, fines and sanctions against the employee, and possibly against the firm and management. It will also likely lead to a cease-and-desist order against the firm.

When building a MNPI compliance program, the biggest challenge a firm may face is dealing with different systems and none of them speaking to one another. There is no aggregator. Sure, Compliance may have access to all of them, but the compliance analyst must constantly swivel from one monitor to another.

Today, software can be the aggregator. The project-data centralizer. This is exactly what it sounds like: a system that gathers as much deal-related information as possible into one place, through integrations. Good MNPI software means easy integrations with existing firm systems, including CRM, human resources, market data, and research systems. All of this adds up to simplified analysis of the project data required to keep a close eye on activities, which translates into faster, safer decision making and less firm risk.



Centralized, Comprehensive Collection of MNPI

Modern MNPI software should integrate with existing employee conflicts monitoring suite and CRM applications—giving Compliance teams the widest possible view of employee activity, and the clearest possible insights into potential conflicts and MNPI flow. On the employee side, good software offers users a portal through which they can self-report and update projects and MNPI they've received. Thus, Compliance will immediately be made aware of any employee-surfaced, or project-associated MNPI.

From a Compliance perspective, this process works similarly. MNPI software can provide employees an easy way to report and record any MNPI they've received, giving Compliance the information required to update Watch and Restricted Lists in real-time from a single, centralized comprehensive solution.



Easier Information Barrier Management

Modern MNPI software makes management of the information barriers themselves radically easier. It means easier identification and tracking of employees by role, location, and whether they're public or private-side employees. It means an easier time granting and monitoring access to system and deal files. It means an easier time securely linking information to Watch and Restricted Lists—on a global basis if necessary—and updating that information in real time. And finally, it means an easier time maintaining the Insider List for those subject to MAR.

With software one can maintain lists of employees and third-party contacts who hold MNPI and would be considered insiders against a project. Compliance can associate entries down to the project level and type of required restriction and eliminate duplicative data entry by publishing lists to downstream systems that MNPI software has integrated with.

5

The Future of MNPI Process

No one has a crystal ball, but as we look forward, we expect the level of regulatory and technological change and political volatility to continue. Regulators will inevitably continue to crackdown and introduce regulations to prevent MNPI abuse, placing ever increasing pressure on Compliance teams that are already stretched to their limits.

For instance, we anticipate [further regulations on crypto assets](#) and new use cases involving artificial intelligence (AI) and large language models (LLM), all of which will impact Compliance teams' management of MNPI.

That's why it's imperative to think about these next considerations which offer a starting point to introduce hybrid working controls in your MNPI processes:

- Develop repeatable workflows that adhere to regulatory guidelines.
- Determine how to maintain the synergies you once had while in the office through alternative means of communication. These processes should be built into the workflows.
- Work with all necessary data to do the job, e.g., firm, customer, and employee trades.
- Establish clear and easily repeatable pre-clearance processes.
- Having a tool that can be configured to address regulatory changes or business models is critical. For instance, firms need solutions that address new rules or amendments (e.g., Rule 10b5-1, Reg M or MAR).
- Finally, firms should look for solutions that are flexible enough to deal with mergers, acquisitions, geographic expansion, or new business groups.

In summary, compliance no longer needs to be so complicated. If it's time to retire the 'swivel chair' and elevate your MNPI processes, contact StarCompliance and let us know how we can help.



Contact Us

To find out how StarCompliance's future-ready technology solutions can help build your organization's culture of employee compliance.

www.starcompliance.com

info@starcompliance.com

US: +1 301 685 0490

UK: +44 (0)20 3838 0763