Protecting Firm and Client Information: MNPI and Client Confidentiality

Craig Barrack – Citi
Marla Moskowitz-Hesse – Credit Suisse
Lee Richards – Richards, Kibbe & Orbe

Moderator: Patrick Cox – LPL Financial

I. ESTABLISHING INFORMATION BARRIERS – WHEN AND WHERE

A. Background

1. In its 2012 Summary Report on Examinations of Information Barriers: Broker-Dealer Practices Under Section 15(g) of the Securities Exchange Act of 1934" (which is attached hereto) the SEC Staff provided the following basic background:

> In many instances, broker dealers may receive nonpublic information regarding their clients and market events as part of their business operations, including financial advisory, origination, and trading activities, often under circumstances in which a duty of trust and confidence may be owed to the client or an involved party. When nonpublic information is material, Exchange Act Section 15(g) requires that registered broker-dealers establish, maintain, and enforce written policies and procedures reasonably designed, taking into consideration the nature of their business, to prevent its misuse in violation of the securities laws by the broker-dealer or its associated persons. Such misuse may occur through, among other activities, insider trading prohibited under Exchange Act Section 10(b) and Rule 10b-5; through trading during a tender offer in violation of Exchange Act Rules 14e-3 and 14e-5; or through issuance of a research report based on MNPI. Such policies and procedures created to prevent misuse of MNPI are commonly referred to as "information barriers."
>
> Other federal securities laws may impact information barriers in place at broker-dealers. Section 204A of the Investment Advisers Act of 1940 (the "Advisers Act") places similar obligations on registered investment advisers. Because broker-dealers may be dually registered as investment advisers or may be closely integrated with an affiliated investment adviser (as were most broker-dealers reviewed by the staff), broker-dealers may need to consider the specific challenges such circumstances present in designing their controls. In addition to Exchange Act Section 15(g), broker-dealers may have information barriers programs in order to rely on an exception or affirmative defense found elsewhere in the federal securities laws.

2. The report went on to describe its previous 1990 report:

> In November 1988, ITSFEA was enacted, adopting Exchange Act Section 15(g). In March 1990, the Division of Market Regulation issued a report, "Broker-Dealer Policies and

Procedures Designed to Segment the Flow and Prevent the Misuse of Material Nonpublic Information" ("1990 Report"). The 1990 Report provided an overview of then-current broker-dealer information barrier practices and identified common practices, including the maintenance of watch and restricted lists and the accompanying review of employee and proprietary trading, written procedures, and documentation of reviews.

Information barrier programs, as described in the 1990 Report and as currently observed by the staff, have certain common features: employee training in legal and firm requirements; review and restrictions on trading; physical barriers; formal over-the-wall procedures prior to sharing information with public-side employees; and surveillance. The basic practices and procedures described in the 1990 Report have provided a framework to which enhanced information barriers have been added as business models and business tools have changed. The 1990 Report described practices that raised concerns, and the staff's current examinations generally found that the concerns have since been addressed by the broker-dealers examined – creation of more formal training programs, greater documentation when employees are brought over-the-wall, and significantly increased broker-dealer compliance staff involvement in determining what matters are to be added to the watch list.

B. The reasons for establishing information barriers are as many and varied as the services, and transactions that are provided by financial institutions where client confidentiality is important. The reasons go beyond just those mandated by the securities laws and include many transactions or services in which the firm's client has a significant interest in confidentiality.

1. The attempt to create a definitive, exhaustive list is dangerous (if not impossible), because it might preclude traders, bankers, lawyers and compliance folks from thinking broadly and creatively about the unique, everchanging nature of the products, services and transactions offered by the financial institutions they serve.

C. That said, in the SEC's 2012 Report (attached hereto), cases he SEC has brought over the last decade and general firm practices provide a list of <u>some</u> of the transactions and other services that often require the establishment of a barrier. They include:

- <u>Definitive Client Interest</u>: The Firm has been asked to provide a specific transactional proposal, or a client has asked ICG to provide additional specific information based on a pitch;

- <u>Counterparties</u>: A specific potential counterparty has been identified, or

the Firm becomes aware of a client that has engaged in substantive conversations with another party regarding a transaction;

- Potential Merger or Acquisition: The Firm has been asked to provide financial advisory services or financing for a merger or acquisition;

- Private Equity Activity: The Firm has received information about a potential target either through pitching, advising, or financing a private equity or LBO firm;

- Potential Purchase or Sale of Assets: The Firm has obtained nonpublic information about a significant purchase or sale of substantial or key assets, or has learned of significant positive or negative developments in the negotiations relating to such a transaction;

- Material Financing: A client is seeking financing that is likely to be material to tradable securities;

    - Firms providing financing may have access to MNPI through the following contact points, among others:

        - As administrative agent (usually through the loan origination function, which is frequently within Investment Banking or Capital Markets),

        - As syndicate member (through the loan origination function or Loan Sales),

        - As holder of interests in the loan purchased during orientation (through the loan origination function, Credit, or a special purpose group),

        - As manager of the Loan Site (as administrative group),

        - As loan trader (trading group or principal investment area of the broker-dealer),

        - As Loan Site Monitors for public-side groups to monitor information coming through the Loan Site, and

        - As a member of the bankruptcy committee if the loans default.

- Corporate Banking: Generally, the Firm's Corporate Banking team will have access to its clients' nonpublic forecasts and projections, and may also receive other nonpublic information.

- Underwritings: The Firm is likely to have any role in a potential underwriting or has obtained nonpublic information about a proposed public or private securities offering;

- Securities Offerings: When the Firm is aware of a public securities offering, that is reasonably likely to occur, even if the offering itself may not be MNPI;

- Derivative Sales: For example, a corporate client may want to enter into foreign derivatives if it expects to have income or liabilities accrued outside the U.S. that must be converted into dollars. As a result, Derivative Sales may obtain MNPI, such as unannounced earnings, from corporate clients through its business interactions.

- Share Repurchasing Programs for corporate clients.

- Municipal Securities Division/Public Finance: When the Firm is aware of a tender offer, advance refunding, repurchase program, or new offering that may affect the price of outstanding issues, in the municipal securities context, or has otherwise obtained MNPI in the municipal securities context;

- Bondholders'/Creditors' Committees: A division within the Firm wishes to participate on a creditors' or bondholders' committee (whether ad hoc, formally or informally organized, and whether public or private);

- Research: The Firm's analyst is preparing a report with a significant rating change or other assertion.

- Proprietary trading by the Firm.

- The receipt of significant orders typically from institutional clients.

- The receipt of orders or information from corporate insiders.

D. This is far from an exhaustive list. For example, firm employees may learn in various ways about changes to senior corporate management or boards, changes in dividend policy, or significant changes in a firm's business, its indebtedness, its plans for expansion or curtailment or changes in its licensing or posture with regulators.

1. In the end, common sense will most often be the best guide in determining how to handle sensitive and/or confidential information.

E. Recognizing and Acting on MNPI

1. Most firms rely on three lines of defense.

a. The first, and arguably most important, is the business. If policies and procedures are clear and the business folks are well-educated on the rules, the firm relies on bankers and traders as the principal employees for identifying whether transactions they are working on or services or trading they are performing have yielded MNPI.

b. The second line of defense is commonly called the Control Group which serves as the repository of information thought to be material and non-public from all corners of the Firm, and establishes and monitors the various lists of securities that are the subject of that information (e.g., restrictive and grey lists).

c. And the third line of defense are legal, compliance and risk personnel.

II. ELEMENTS OF EFFECTIVE INFORMATION BARRIERS

A. Once again, given the many and various types of MNPI firms receive, it is not possible to provide an exhaustive compendium of effective barriers and other means of preventing the inappropriate sharing or use of MNPI and other confidential client information.

B. But the attached SEC 2012 Report gives useful guidance on some of the methods the Staff expects to see, such as:

1. Monitoring Lists

- Firmwide Restricted Lists
- General Surveillance (Grey or Watch) Lists
- Hybrid Restricted and Surveillance Lists

2. Limiting Authorized Access

- To Deal Team Members and other Private Side Personnel
- And to the Control Room

3. Controlling Access for Public Side Dual Function Employees, e.g. members of Commitment Committees.

4. Physical Barriers

5. Monitoring and Educating Private Side Employees with respect to Informal Discussions with the Public Side.

6. Technology Barriers

7. Controlling Information Access to Printing and Production Employees

8. Disposal of Confidential Documents.

9. Policing of Wall Crossings

- Pre-approval by Compliance
- Using Supervisors to effect the Crossing

10. Policing Access to Electronic Websites such as Loan Sites and Data Rooms

11. Policing Information Received Pursuant to Confidentiality Agreements

12. Monitoring or controlling contacts with Institutional Investors

13. Employee Pre-Clearance Requirements

14. Email controls and reviews

15. Surveillance of trading in all potentially affected securities including lookbacks and pattern surveillance

III. SHARING CONFIDENTIAL INFORMATION

A. Once confidential information (whether or not it is MNPI) is received the default established by most firms is to provide that it be shared internally only on a "need to know" basis within the Firm and only with those who will protect its confidentiality, and not shared outside the Firm.

1. There are, of course, exceptions to the prohibition against sharing confidential information outside the Firm including:

a. In connection with execution or facilitation of a particular transaction, specific transactional information (such as quantity, price parameters, security type) may be shared where necessary for the execution or facilitation of the transaction.

i. The client's identity is not shared and the information shared will not reveal that identity;

ii. Sharing will not be adverse to the client's interests; and

iii. The sharing is not contrary to an agreement with the client.

b. Communications regarding trader views of markets or "market color" and thoughts about risk management such as the directions of possible trades or approximate exit or entry points.

i. Market color is obviously a broad and fuzzy topic, but it generally includes levels of market prices, volumes and directions, so-called "flows," and trading strategies, for example strategies based on macro-economic, technical or fundamental observations. Particular client "flows" may, under some circumstances, be shared where the identity of the client is protected, the information is appropriately general and the sharing would not adversely affect the client.

c. Communications with regulators, law enforcement or self-regulatory bodies subject to compliance or legal approval, with parties pursuant to appropriate non-disclosure agreements, or with parties owning fiduciary duties (such as lawyers and auditors).

2 The "need-to-know" standard is naturally somewhat amorphous and must be determined based on common sense on a case-by-case basis.

a. Some obvious examples of personnel who might "need to know" particular information include

i. Relevant trading and sales desks acting for the benefit of the client;

ii. Support staff assisting in booking, executing, settling and clearing particular transactions;

iii. Supervisors

iv. Functional areas of the Firm such as Operations, Legal, HR, Risk, Finance, the Control Room, other compliance personnel, IT and Tax.

v. Employees who generate business metrics; and

vi. Firm traders or other personnel managing the Firm's risk where consistent with normal trading and risk management policies.

3. When the confidential information is deemed to be potentially non-public and material, firms typically erect information barriers or rely on the existing barriers between the public and private sides of the Firm.

IV. IDENTIFYING IMPROPER INFORMATION SHARING

A. In order to identify improper information sharing one must first know what to look for and one guide can be found in the cases brought by the Commission over the last ten years or so.

B. In the Matter of Mizuho Securities USA, LLC (July 23, 2018, Release No. 34-83685)

1. This case concerned information-sharing between two public-side business units, Mizuho's International Sales Trading Desk and U.S. Equity Trading Desk, which were located on the same floor of Mizuho's New York office. The International Desk routinely handled issuer buyback programs for Mizuho corporate customers.

2. Although buyback programs are publicly announced, issuers typically do not publicly share the dates on which they intend to execute trades pursuant to a buyback program. On such dates, buybacks can constitute a significant volume of total trading in an issuer. Nor do issuers announce whether or to what extent they plan to execute the announced program. Accordingly, news that an issuer is planning to execute buyback trades on a particular day constitutes confidential customer order information which may be useful to other market participants:

    a. It provides understanding "of the manner in which the stock is likely to react to eh buyback trading, given the size of the buyback activity or the fact that there is buyback activity supporting the stock price"; it allows market participants to refine their earnings estimate models; and it provides insight into intraday price and volume movements.

3. Mizuho's International Desk shared information regarding daily buyback activity with the U.S. Desk, even though almost all buyback trading occurred through an algorithm without the involvement of the U.S. Desk. Before market open, the International Desk would send buyback information including order size and the limit price to the U.S. Desk, and also placed the information on an order management system that the U.S. Desk could access.

4. U.S. Desk sales traders shared this confidential buyback information with other Mizuho customers.

5. After Mizuho learned that the SEC was investigating, Mizuho terminated U.S. Desk access to the International Desk's order management system and moved issuer buybacks to another, private-side desk. It also implemented new trainings and procedures. Mizuho was assessed a $1.25 million civil penalty.

C. In the Matter of Deutsche Bank Securities, Inc. (October 12, 2016, Release No. 79083)

1. Deutsche Bank Securities, Inc. (DBSI) was censured for several distinct but related issues concerning information-sharing between equity research analysts and customers, and between analysts and traders. The SEC

developed two themes—written policies that contained gaps or loopholes which analysts exploited, and written policies that were not adequately supported by monitoring from compliance staff.

2. DBSI allowed analysts to speak directly to customers and compensated analysts in part based on customer assessments, which created an incentive for analysts to provide additional information to customers. DBSI prohibited analysts from sharing "research in process" with customers or anyone else outside of the research department. DBSI also required that any material change in view be published online. But the SEC identified inadequacies in these policies that allowed analysts to share MNPI with particular customers.

    a. First, the definition of "research in process" extended to when the analyst "has definitely decided to publish a report and has a developed thesis for that report." Analysts used this definition to share new ideas with customers even as they were drafting a new research report, so long as they did not have a developed investment thesis for that report. But the underlying ideas, even without the conclusion, could still constitute MNPI.

    b. Second, the SEC found that DBSI set too high a bar for finding materiality. Although a rating or price target change was always material, an estimate change was considered material only when it was greater than 10%. The SEC concluded that an analyst's change in estimate of quarterly or annual financial performance by less than 10%can be, and often is, highly relevant to the average investor.

    c. Third, DBSI required analysts to publish short-term trade ideas, which were defined as trade ideas that an analyst believed would be valid for at least two weeks. These could be published even if they differed from an analyst's long-term rating of a stock. But there was no policy that governed trade ideas of less than two weeks. The SEC found that some analysts told individual customers to "get out," "short," and even "puke" stocks for which the analysts had a published HOLD rating.

        i. Although DBSI did have a general policy that prohibited analysts from selectively disclosing any trading idea that was inconsistent with their published ratings, the SEC found this policy to be inadequate.

3. DBSI also allowed analysts to share trade ideas with sale staff and traders with inadequate monitoring, which created a risk that analysts would disclose unpublished market sensitive information in violation of DBSI policy. Similarly, DBSI allowed analysts to meet with customers at "idea

dinners" hosted by the firm—again, with inadequate monitoring from compliance.

4. DBSI was assessed a $9 million civil penalty.

D. In the Matter of Wells Fargo Advisors, LLC (September 22, 2014, Release No. 73175)

1. This case concerned insider trading by a Wells Fargo broker on the basis of MNPI that the broker obtained from one of his customers. The SEC found that Wells Fargo's compliance policies were inadequate to deter or detect such insider trading. Of particular concern was the fact that Wells Fargo compliance reviewed the trade at issue, identified potential red flags, but then closed the investigation without further inquiry or escalation.

2. A Wells Fargo broker learned from a customer, who was also invested in a private equity firm, that the private equity firm intended to acquire the fast food chain Burger King. The Wells Fargo broker traded on that material non-public information, making $175,000 in ill-gotten gains. He also tipped others—including other Wells Fargo brokerage customers—who also traded ahead of the announcement.

3. In the course of the SEC's investigation of the insider trading, it determined that Wells Fargo had stated in internal documents that its compliance policies were inadequate to detect the acquisition of MNPI from customers, but nevertheless failed to implement adequate policies. And although multiple compliance groups looked into the broker's trading in Burger King, they failed to coordinate, failed to elevate the issue to senior management, and missed what the SEC determined to be "several red flags" that the broker was engaged in insider trading.

4. It's clear that Wells Fargo was in some respect the victim of bad luck—they likely would not have gotten a close look from the SEC were it not for their broker's insider trading. But their compliance function was nevertheless significantly flawed during the relevant time period.

   a. Compliance was slow to conduct lookbacks and developed a backlog of as much as 10 months.

   b. Compliance failed to consistently follow up on or escalate the red flags that they identified, if they deemed them unimportant.

   c. And, most critically, compliance failed to keep records of the lookbacks that resulted in a statement of "no findings." There was no paper trail for the SEC to review—and no evidence that Wells Fargo could point to showing that compliance was in fact implementing firm policies.

5. When the Burger King acquisition was announced, compliance reviewed the broker's trading and determined that he had traded in the stock within 10 days of the announcement; that he was located in the same city as Burger King; and that he, many of his customers, and the private equity fund acquiring Burger King were all Brazilian nationals. Despite the presence of these red flags, compliance did not investigate the broker's trading.

6. Wells Fargo was assessed a civil penalty of $5 million for its compliance failures.

    a. It is not clear that Wells Fargo could have implemented an information barrier that would have prevented its broker from learning about an acquisition from a customer. But detection of suspicious trades is a critical part of deterrence. No information barrier will be sufficient if compliance is asleep at the switch.

E. In the Matter of Goldman, Sachs & Co (April 12, 2012, No. 34-66791)

1. This matter concerns information-sharing between equity research analysts and traders at Goldman Sachs. Goldman failed to implement clear policies distinguishing between what analysts could and could not share with traders, and failed to maintain robust compliance monitoring of meetings between them.

2. Goldman Sachs instituted a weekly "huddle" program. At the huddles, which were divided by sector, equity research analysts would meet with traders to discuss "commercially oriented trading ideas." Goldman also developed what it called the Asymmetric Service Initiative, in which analysts disseminated the ideas discussed at huddles directly to a selected group of hedge fund and investment management clients (who were selected because they provided the firm with a high volume of trading commissions).

3. For two years, Goldman did not develop any new compliance policies to govern what could and could not be discussed at huddles. The existing policy prohibited research analysts from discussing unpublished research with anyone outside of research (other than compliance and legal). Goldman eventually updated its policy to require that during huddles analysts not "engage in selective disclosure of unpublished research or indicate pending changes in ratings."

4. But the SEC found that this is precisely what happened at huddles. Through its investigation, the SEC uncovered hundreds of examples of an analyst changing their public long-term rating of a stock within five business days of discussing the stock at a huddle. To give just one example, in April 2008 an analyst covering a company drafted, but did not

publish, a research report upgrading a company from Neutral to Buy. The analyst highlighted that company during a weekly huddle and, later that day, recommended the upgrade consistent with his report. Four days later, Goldman upgraded the public rating.

5. The SEC also found that Goldman was not adequately monitoring the huddles for potential disclosure of MNPI. Compliance staff only sometimes attended the huddles. And Compliance never undertook an internal investigation to determine whether analysts were disclosing upcoming rating changes to traders or firm clients. The SEC found some serious red flags here that Goldman should have looked into—including an employee evaluation in which an analyst was admonished for disclosing impending rating changes to clients. The SEC also found that compliance failed to keep adequate records of the investigations were undertaken.

6. Lastly, Goldman failed to conduct trade surveillance that was reasonably designed to ensure that analysts were not prematurely disclosing material research changes to traders and clients. Trade surveillance was not made aware of when stocks were discussed in a huddle, and eventually relied on an algorithm-driven surveillance system focused on the profitability of trading that simply ignored suspicious trades that netted less than $650,000 in potentially illicit profits.

7. Goldman was assessed a civil penalty of $22 million—$11 million to the SEC and $11 million to FINRA in a related investigation.

F. In the Matter of Merrill Lynch (March 11, 2009, Release No. 59555)

1. Finally, we have another case concerning the failure of a broker-dealer to prevent bad-actor employees from willfully sharing MNPI for the employees' personal benefit. The SEC attributed a front-running scheme operated by certain Merrill Lynch brokers to lax compliance policies at Merrill Lynch, which were inadequate to prevent or detect the improper information-sharing.

2. Merrill Lynch used an "equity squawk box" system to disseminate customer orders from brokers to traders. Merrill Lynch did not have any written policies to govern who had access to the squawk box or to monitor the use of the squawk box.

3. As a result, some Merrill Lynch retail brokers were able to obtain squawk box information even though they had no bona fide need for it in their business. Instead, they sold the squawk box information to day trading firms by putting an open phone line next to the squawk box. As large customer orders came in, the day traders were able to front-run the orders and turn quick profits. The day trading firms then paid kickbacks to the

retail brokers who provided access to the non-public order information.

4. Merrill Lynch had policies in place prohibiting insider trading and front-running, but that was not good enough for the SEC. What mattered here was that misconduct occurred and that Merrill Lynch had no way to monitor or prevent it.

   a. The SEC order requires increased training, supervision, and the placement of "signs on all equity trading floors reminding employees that customer order information is confidential." Which suggests that the SEC also did not have a great idea how to manage squawk box access.

5. Merrill Lynch was assessed a civil penalty of $7 million.

G. As noted above, the SEC has stressed the need to establish effective surveillance of trading in all potentially-effected securities and surveillance of employee communications.

1. The Staff observed in the 2012 Report that

> "[a]t the most basic level, most broker-dealers conduct random samplings of emails to identify potential concerns. Some broker-dealers have targeted reviews for when an "internal use only" document is sent outside the broker-dealer or for large attachments sent to generic internet email domains. Some broker-dealers will conduct ad hoc email reviews when surveillance identifies concerns in trading or following on announced deals." Id. At 37.

2. It also stressed that reviews should include related derivatives like credit default swaps, stock futures, equity or total return swaps, warrants and bond options. Id. at 39.

3. And the Staff has emphasized the need to do historical lookbacks to search for suspicious patterns of trading, even in trading of securities the Firm did not represent.

V. WHAT TO DO WHEN YOU FIND A BREACH

A. The response to a breach will obviously depend on its seriousness and whether it was intentional or not. However, in all cases it is important to involve legal and/or compliance in the inquiry.

B. In the case of serious breaches of MNPI, the playbook is relatively simple.

1. An investigation must be done, presumably led by in-house or outside counsel. Involving counsel will protect the investigation and its results

under the attorney-client privilege.

2. The aim of the investigation is to understand the origins and the full nature of the breach, the damage, if any, done by the breach, and whether it was intentional.

3. The answers to those questions will allow the Firm to

- Take the necessary remedial steps to avoid any similar breach in the future;
- Decide whether any clients need to be notified and, if necessary compensated;
- Make any necessary personnel decisions, including on the issue of whether employees need to be suspended, disciplined or terminated; and
- Decide whether to report the breach to any regulator.

C. The SEC staff has emphasized the importance of documenting the firm's investigations and the effectiveness of its surveillance so that the Staff can better judge the Firm's review.

D. It has also warned against relying heavily on the accounts of the employees who are the subjects of the review.