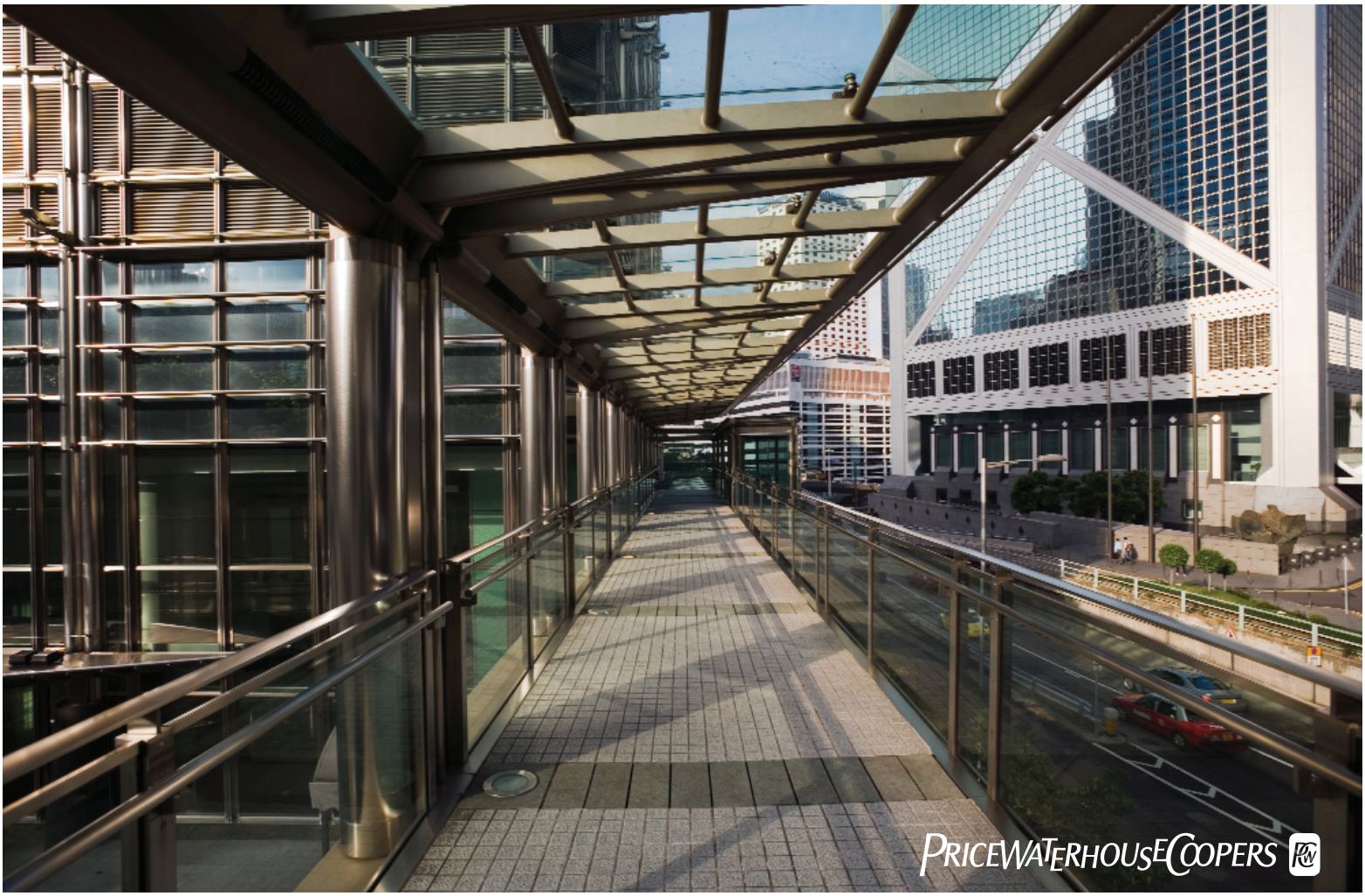
Financial Services Regulatory Practice

Private fund advisers

Integrating testing into a risk-focused compliance program



Contents

The financial services industry that has emerged from the recent market turmoil is one that has stricter standards, greater regulatory scrutiny, and higher client expectations for alternative asset management firms. As part of the Dodd-Frank Wall Street Reform and Consumer Protection Act many hedge fund and private equity fund advisers (private fund advisers) will be required to register with the Securities Exchange Commission (SEC). Those that register will be subject to the same rules, regulations, and requirements as traditional advisers, including having to implement and annually assess a compliance program as mandated by the Investment Advisers Act Rule 206(4)-7.

In order to become compliant with the Investment Advisers Act Rule 206(4)-7, chief compliance officers (CCO) and the compliance professionals of registered private fund advisers will be required to develop a compliance program and implement compliance policies and procedures. In addition, implementation of an accompanying testing framework will be critical in assessing the effectiveness of the policies and procedures as well as in assessing the overall firm-wide compliance program. The SEC has stated that the policies and procedures that underpin an adviser's compliance program "should be designed to prevent violations from occurring, detect violations that have occurred, and correct promptly any violations that have occurred."[1] Although the SEC has not mandated particular tests, it has signaled through recent exams, staff speeches, and the 2004 compliance program rule that "compliance policies and procedures should employ methods of detection by using compliance tests that analyze information over time to identify unusual patterns."[2]

More than ever, CCOs and compliance professionals will need to understand their firm's business and become knowledgeable about its operations. This knowledge will be critical in defining compliance objectives and requirements, assessing areas of their firm where compliance activities are needed, and implementing effective and statistically significant tests to yield the most relevant results. While this involves a strong understanding of roles and responsibilities, and well-defined compliance processes, the testing effort can be greatly supported through technology. Compliance professionals should employ technological tools wherever possible so that they can focus on analyzing results and identifying potential compliance program violations, rather than performing manual calculations, which can be time-consuming and far less effective.

The compliance program and its associated testing framework should reach across the firm and not only cover Investment Advisers Act requirements, but also adjust to the regulatory climate as new issues arise and become focal points of the SEC. As the new financial services industry continues to take shape, advisers, including private fund advisers, should consider several top risk areas when developing a compliance program and testing framework. This paper discusses the development of a compliance program and testing framework to address these top risk areas and will suggest ways in which technology can assist in this process.

1 *Compliance Programs of Investment Companies and Investment Advisers* (17 CFR Parts 270 and 275, Release Nos. IA-2204 and IC-26299, December 17, 2003), IIA.1.paragraph 3
2 *Compliance Programs of Investment Companies and Investment Advisers* (17 CFR Parts 270 and 275, Release Nos. IA-2204; IC-26299; December 17, 2003), Footnote 15

Tailoring the compliance program

A firm's CCO and compliance professionals should design a compliance program that aims to identify, assess, and monitor compliance risks associated with the firm's particular investment activity. As a first step, they should undertake a diligent assessment of their firm. Private fund advisers should consider the following elements when determining whether their compliance program is appropriate for their business:

- **Definition of objectives**: Clearly define the objectives of the private fund adviser's compliance program and the roles and responsibilities of various business and support functions.
- **Assessment of the enterprise**: Consider the types of clients that the private fund adviser oversees, the types of services offered, the types of products that the adviser manages, and the strategies and instruments that those products employ.
- **Assessment of risks**: Identify and assess real, potential, and apparent conflicts of interest, inherent business risks, and developments in the regulatory and financial services environment that are associated with the firm. As changes occur in the adviser's operating and regulatory environment, the associated conflicts and risks should be reevaluated and adjusted accordingly.
- **Development and implementation of compliance policies and procedures**: Develop compliance policies and procedures to address enterprise-wide conflicts and risks. Firms should communicate and distribute compliance policies and procedures to its employees and redistribute them periodically through compliance training.
- **Development and execution of a testing framework**: Develop and execute targeted tests to identify indications of violations and to assess the effectiveness of the compliance program in mitigating compliance risks.

Testing: Its role in the compliance monitoring function

Development and execution of a testing framework is integral to the surveillance of an adviser's compliance program and to the detection of violations of the firm's policies and procedures. Testing not only provides tangible insight into whether compliance control objectives are being satisfied, but also can provide insight into trends and patterns that occur over time. Compliance program tests should not only be designed to mitigate particular compliance risks but also be modeled around the four established types of testing: inquiry, observation, examination, and re-performance. Further, all of these types of tests can occur on a periodic (monthly, quarterly, annually) or real-time basis. Technologies have evolved to provide real-time, or near real-time, monitoring as a means of detecting compliance issues early and addressing them before they become significant.

Testing should be targeted toward high risk areas and can be viewed as both transactional and forensic in nature; both types of testing are important in compliance testing. Transactional tests assess the accuracy and completeness of daily transactions, such as allocations of daily expenses to funds and authorization of trades. Forensic testing takes a deeper look into data and provides broad perspectives that might not be available through investigating individual transactions. The objective of forensic testing is to allow the data to tell a story about the firm's practices that might identify adverse trends and patterns over time. Forensic testing helps the CCO determine whether such trends are indicative of a potential compliance violation or, worse, fraudulent activity.

Use of technology in the testing framework

Forensic and transactional testing requires data from various systems that are being used across the enterprise. Expense processing systems, trading platforms, compliance monitoring systems, database repositories, and accounting systems carry historical data that can be used for compliance testing purposes. Compliance professionals should work with those responsible for these firm-wide systems to develop customized access to data that will enable them to get necessary information to perform compliance-related testing.

In business areas where large quantities of data need to be analyzed, compliance controls and associated testing will rely heavily on the integration of current technology or new tools to mine vast amounts of data, identify correlations between multiple data points, and perform testing in a timely manner. Automation of testing is essential in helping asset managers achieve a scalable and sustainable compliance infrastructure; testing cannot be efficiently performed through manual procedures alone. In developing tests, private fund advisers should assess their information technology (IT) systems to determine their ability to support the compliance program. While most asset managers recognize the need for more effective compliance technology to replace manual processes or outdated systems, many also find that they do not have the resources, time, regulatory expertise, or knowledge to obtain it. Accordingly, third-party vendor solutions might be necessary to bridge the gap.

When evaluating enhanced technological solutions to assist with the testing and monitoring elements of the compliance program, the adviser should consider the following steps:

- Assess the technology requirements
- Assess current technological capabilities
- Identify gaps in technological capabilities
- Determine whether solutions to gaps can be developed internally or whether a third-party vendor would be better suited to provide solutions
- Identify various vendor offerings
- Determine the appropriate solution and develop a plan for solution implementation

Testing considerations for top compliance risks

The SEC has shifted its focus to address new issues that have come to the forefront of the financial services industry. Certain compliance risk areas are critical for private fund advisers to consider because they have been highlighted by the SEC in recent examinations and enforcement activities. Below are examples of some of the top risk areas for private fund advisers to consider and examples of tests that can act as a first line of defense for compliance departments by leveraging people, processes, and technology across the firm. The following list of examples is not meant to be a complete test inventory but rather provide testing ideas for some of the current focal areas of the SEC. Additionally, the below examples are generic in nature; compliance tests should be tailored to each individual firm.

Insider trading

A regulator's expectation for a robust compliance program would certainly include controls around insider trading. First, an adviser should identify potential sources of material non-public information, and then work to design controls that will serve to detect the potential receipt of material non-public information from each of those sources.[3] A complete compliance program addressing insider trading should be composed of preventive controls that attempt to prohibit insider trading, as well as detective controls designed to identify instances of insider trading.

Material non-public information can come from a number of potential sources, both internal and external to an adviser's business. For this reason, identifying potential sources of material non-public information and designing controls around insider trading should be undertaken across all aspects of an adviser's entity.

Particular attention should be given to those potential sources of material non-public information where there is a mutual interest. For example, whenever there is an economic tie such as a personal investment, or an existing employee relationship with a corporate insider or investment professional, the likelihood of the exchange of material non-public information increases. In such instances, compliance should consider developing an automated email surveillance program to detect communications between firm employees and others who might have material non-public information (e.g., between a firm trader and an outside broker). Similar email surveillance for communications with former employers and disclosed personal relationships with corporate insiders should be performed. Email identified in this automated surveillance should be flagged for further review.

3 SEC Rule 10b5-1 clarified that the prohibition against insider trading does not require proof that an insider actually used material non-public information when conducting a trade; possession of such information alone is sufficient to violate the provision.

The complexities and abundance of potential sources of material non-public information within an adviser's business emphasize the need to dedicate more resources and technology in this area, as there is no more pressing compliance risk for an investment adviser to address.

Institutional conflicts

The compliance function within an organization should be aware of situations in which advisers are conflicted with the client accounts that they manage, or situations in which advisers could benefit at the expense of clients. After identifying any such situations, compliance departments should draft clear policies to mitigate potential conflicts and develop controls to monitor the identified conflicts.

A common area of conflict is trade allocations among accounts. In designing controls around trade allocations, compliance professionals should first develop an allocation policy that provides for fair and equitable allocations of trades across all client accounts. Any trades requiring non-standard allocations should be formally memorialized and approved by the CCO and applicable supervisory personnel prior to trading. Customized reporting can be created using trade data from order management systems or from internal portfolio accounting systems to test trade allocations. On an ongoing basis, using automated surveillance, the allocation methodology applied to trades should be compared to expected allocations prescribed by the allocation policy. Additionally, automated surveillance can be designed to identify trends where profitable trades appear to be continuously weighted to accounts with larger amounts of affiliate capital or higher fees. Any adverse trends that might indicate unfair allocations should be addressed immediately with the portfolio management team and trading desk.

Cross trading, another institutional conflict, can be monitored by designing systems to perform an automated scan of all transaction activity. In designing such automated surveillance, compliance should consider opposite-direction trading across the organization in the same security, on the same day. Additionally, parameters should be designed to consider instances in which a security is directly traded from one account to another. Any identified instances of cross trading should be investigated to ensure they are consistent with firm policy, that documentation evidencing the approval and rationale for such trading was prepared prior to execution, and that the executed trade price represents fair value. Then, all cross trades should be reviewed for patterns indicating favoritism or other abuse.

Valuation

The SEC stresses the importance of establishing an adequate control environment that ensures independent and accurate fair value measurements to protect investors. An adviser has the responsibility to develop a structured approach to valuation that includes gathering relevant and observable market information and applying reasonable judgment in deriving a value that represents the best estimate of the current exit price for an asset.

With the use of automated controls, an adviser can address some of the risks associated with valuation and more easily identify positions that call for further investigation. For instance, an adviser could monitor for any illiquid or stale-priced security that sold for more or less than 3 percent of the last marked price and automatically flag those instances. Such occurrences might indicate improper valuations in prior months and, hence, merit further investigation. Automated surveillance also can be designed to flag a security that is marked through a different methodology or that has a different source of support for its value in the current month than it did in the prior month. Once automated, such controls will help to ensure, with little burden on compliance, that such instances are flagged and investigated for reasonableness and are not overlooked when determining fair value.

Personal conflicts and code of ethics

Private fund advisers owe a fiduciary obligation to clients, where the interests of clients are always placed before the interest of the adviser or its employees. Because it helps the adviser to carry out its fiduciary duty, administering a code of ethics for the adviser and its employees is a critical compliance function.

A key aspect of a code of ethics is establishing controls around employee personal trading. Employee personal trading presents significant potential for abusive practices such as front-running, cherry-picking, insider trading, and scalping. For advisers with a large volume of employee personal trading activity, the responsibility to monitor personal trading can be daunting; however, by using technology, compliance departments can easily gather and analyze vast amounts of employee personal securities transactions to identify improper trades and patterns of improper trading.

Specifically, personal trading monitoring systems should cover all the parameters of the adviser's personal trading policy, which may include minimum market capitalization limits, trade size limits, restricted lists, watch lists, blackout windows, holding periods, and disallowed security types. Additionally, for employee personal trading, companies should issue a list of approved brokers that provide advisers with automated feeds into their personal trade monitoring system; this would enable compliance personnel to easily compare personal trade activity against firm trading activity.

Another key aspect of the code of ethics monitored by compliance personnel is the exchange or receipt of gifts or gratuities between or among parties that have a fiduciary duty to funds and clients. Excessive or otherwise inappropriate gifts or entertainment can be an indication of a potential conflict of interest and can ultimately damage the adviser's reputation. To minimize the risk of personal conflict, compliance should develop ongoing automated surveillance to oversee gifts and entertainment provided to or from third parties and attempt to identify potential correlations to an increase in business activities with such third parties, especially trade activity and commission rates. In addition, while individual gifts and gratuities may be appropriate under the firm's guidelines, compliance should seek to review all gifts/gratuities over a period for any patterns that could indicate a potential problem.

Risk disclosures

A critical obligation of an adviser is to fulfill its disclosures to investors concerning its investment strategy. Within its offering memorandum, and other documents, an adviser generally details the potential risks associated with an investment or a strategy. An adviser should assure that it is conducting its trading and investment activities within its disclosed risk parameters.

For example, compliance personnel can develop surveillance in real time using current trade data to monitor the trade activity and holdings of each of its portfolio managers, as well as the cumulative trade activity and holdings across the firm, to ensure that it is within the firm's risk parameters. For this type of sophisticated monitoring to be effective, it must be automated to facilitate the analysis of multiple aspects of large volumes of data in real time.

Automated surveillance could, at a minimum, analyze trading activity for concentrations in issuer names, liquidity exposures, stop-loss limits, maximum beta limits, and other such parameters. The risk department should report cases in which material risk parameters have been exceeded to compliance personnel, who will document limit breaches and evaluate them further for trends or more serious issues. In addition, the performance results of accounts and funds utilizing similar strategies could be compared, or those with otherwise aberrational performance identified, indicating the possibility that the manager might have taken risks beyond the disclosed risk profile of the account/strategy/fund.

Safeguarding of assets

Safeguarding of assets became a higher-priority risk in recent years, after incidents of theft and misuse of client assets occurred. Advisers have a responsibility to monitor the safety of the assets they manage this includes monitoring expenses charged to investors.

Technology can play a valuable role in helping compliance departments monitor expense allocation. For example, the establishment of an automated alert mechanism within an accounting system can notify advisory personnel when actual fund expenses are significantly exceeding expected expense, management, or incentive fee ratios stated in fund offering documents. Similarly, an alert can be sent to advisory personnel when disbursements from funds are made to unapproved vendors or are made without proper authorization. Compliance departments can leverage results of these expense alerts by periodically checking with the accounting department and investigating any instances of adverse activity.

Market manipulation

Market manipulation can be defined as a deliberate attempt to interfere with the free and fair operation of the market and create artificial, false, or misleading appearances with respect to the price of a security. Manipulative behavior continues to evolve along with the markets; however, manipulation often takes the form of false or misleading rumors designed to influence others to trade in a particular way, or buy and sell orders designed to affect prices or turnover in order to create an opportunity for profit.

Market manipulation, like insider trading, can be difficult to identify and prevent, but that does not exempt an adviser from its responsibility to build a strong control environment designed to prohibit, detect, and discourage manipulative trading activity. Without the integration of intelligent, automated procedures, the search for potentially manipulative trading is like searching for a needle in a haystack.

To identify manipulative behavior, advisers must work to implement automated surveillance that can strategically analyze trade output and flag patterns for further investigation. Although every adviser's business is unique and surveillance procedures must be tailored to suit the activity of each individual adviser, one useful test is to automate a post-trade surveillance procedure to identify instances in which an adviser's trade volume makes up a significant portion of an issuer's total trading volume; such instances present an increased likelihood of manipulative trading behavior and should be further investigated. Another effective automated procedure to consider is one designed to flag instances in which the firm simultaneously trades in opposite directions across the capital structure of an issuer, including derivative trades for which the reference entity is the issuer.

Regulatory filings

Alternative funds have large equity interests in an issuer that trigger reporting requirements to the SEC. It is important for compliance departments to closely monitor equity positions held by their funds and by their executives to accurately and timely report beneficial ownership.

Trading in issuer names can be reviewed daily as positions approach reporting requirement limits simply by using automated surveillance techniques. When near a limit, such issuers can be placed on a watch list so they can be more closely monitored. When reporting limits are reached, an automated alert can be sent to a centralized compliance calendar with built-in reminders as reporting deadlines approach. Using automated surveillance in this area of regulatory filings will eliminate the potential for human error and result in an effective control while simultaneously reducing the burden on compliance to manually monitor trading activity and reporting deadlines. Another effective test involves isolating all incidents in which reporting thresholds were reached and identifying the associated filing for each one.

Investment guidelines and restrictions

When advisers set restrictions in their offering documents such as the intention to stay within a certain position, industry, or sector concentration limit, they are obliged to implement a monitoring framework to adhere to those restrictions. Likewise, if clients require specific investment guidelines, advisers must ensure those are adhered to as well.

Compliance departments can monitor investment guidelines and restrictions on a post-trade or pre-trade basis using relevant technologies. Post-trade monitoring is standard industry practice, but the leading industry practice is to monitor investment guidelines and restrictions on a pre-trade basis. A number of compliance monitoring modules can be added to trade order management systems or accounting systems for which portfolio guidelines and restrictions are monitored as transactions occur. As trades in securities are entered into the order management system, alerts can be sent to compliance and trade executions can be blocked in issuers that are approaching or meet a limit. In these instances, guidelines and restrictions are monitored on a real-time basis with the intent of preventing a breach before it happens.

Compliance professionals should also continuously monitor firm offering documents and marketing materials for any changes to investment guidelines and restrictions and ensure that any changes are integrated into the monitoring mechanism.

Other examples of forensic type tests for advisers can be found on the SEC's Office of Compliance Inspections and Examinations website.[4]

4 http://www.sec.gov/info/cco/ccons2007.htm

Conclusion

As clients, investors, and regulators place more scrutiny on private fund advisers, and with many private fund advisers coming under SEC oversight for the first time, it is important for their CCOs and compliance professionals to develop effective compliance programs and associated testing frameworks. As part of those testing frameworks, these CCOs will need to determine the proper balance of transactional testing and forensic testing to provide the most insight into their firm's practices. CCOs and compliance professionals also should determine where technology and automation can be utilized effectively to aid in the compliance program testing effort. CCOs must ensure that indications of problems or violations revealed by testing are appropriately investigated and resolved and determine whether such results warrant changes or improvements to the compliance program or training. Lastly, compliance programs and testing should adapt and change so that it remains evergreen as the firm's business, clients, investments, and associated compliance risks change.

Contacts

For more information, please contact:

Tom Biolsi
Asset Management Regulatory Leader, US
New York
646-471-2056
thomas.biolsi@us.pwc.com

Gary Meltzer
Asset Management Advisory Leader, US
New York
646-471-8763
gary.c.meltzer@us.pwc.com

Peter Horowitz
Principal
New York
646-471-3243
peter.a.horowitz@us.pwc.com

Lori Richards
Principal
Washington, DC/New York
703-610-7513
lori.richards@us.pwc.com

Daniel Ryan
Partner
New York
646-471-8488
daniel.ryan@us.pwc.com

David Sapin
Principal
Washington, DC/New York
703-918-1391/646-471-8481
david.sapin@us.pwc.com

Ellen Walsh
Partner
New York
646-471-7274
ellen.walsh@us.pwd.com

Robert Nisi
Managing Director
San Francisco
415-498-7169
robert.nisi@us.pwc.com

Bernie Denis
Director
Washington, DC/New York
703-918-3401
bernard.h.denis@us.pwc.com

Anjali Kamat
Director
New York
610-933-4340
anjali.kamat@us.pwc.com

Kent Knudson
Director
Washington, DC/New York
703-918-1377
kent.knudson@us.pwc.com

A. Duer Meehan
Director
Washington, DC/New York
703-918-6191
a.duer.meehan@us.pwc.com

Stefanie Neches
Director
New York
646-471-4501
stefanie.neches@us.pwc.com

Scott Pomfret
Director
Boston
617-530-7392
scott.pomfret@us.pwc.com

A special thanks to Michael Bacharz and Matthew Nullet for their contributions to this document.

pwcregulatory.com