King & Spalding
Client Alert

Securities Enforcement and Regulation
Data, Privacy and Security

MAY 1, 2018

For more information, contact:

Dixie L. Johnson
+1 202 626 8984
djohnson@kslaw.com

Carrie A. Ratliff
+1 404 572 2801
cratliff@kslaw.com

Michael R. Smith
+1 404 572 4824
mrsmith@kslaw.com

Jeffrey M. Stein
+1 404 572 4729
jstein@kslaw.com

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Keith M. Townsend
+1 404 572 3517
ktownsend@kslaw.com

Dick Walker
+1 212 556 2290
rwalker@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

Practical Advice for Evaluating Insider Trading Compliance Programs in Light of Recent Cybersecurity Events and SEC Guidance

In light of the continuing drumbeat of high profile data breaches and the recent guidance from the Securities and Exchange Commission (the "SEC") to public companies in response (SEC Release Nos. 33-10459; 34-82746, February 21, 2018 ("SEC Cybersecurity Guidance")), many public companies will find it timely to review the operation of their insider trading compliance programs (see our March 2018 Client Alert for more information). The SEC Cybersecurity Guidance serves as a call to action for various stakeholders in public companies – for boards, to evaluate their oversight of cybersecurity risks, and for management, to evaluate the approach to disclosure of cybersecurity risks and incidents, disclosure controls and procedures, and insider trading compliance programs. Just last month, the SEC brought a first-of-its kind enforcement action alleging that a company failed to disclose a cybersecurity breach quickly enough. It is clear the SEC will be monitoring cybersecurity disclosure issues closely in the coming quarters.

In this client alert, we discuss some practical steps that public companies may wish to consider when evaluating their insider trading compliance programs.

1. PURPOSES OF AN EFFECTIVE INSIDER TRADING COMPLIANCE PROGRAM

While there is no specific statute or regulation that requires a public company that is not a broker-dealer or investment adviser to maintain an insider trading compliance policy, following the insider trading scandals of the 1980s and the enactment of the Insider Trading and Securities Fraud Enforcement Act of 1988 ("ITSFEA"), such policies have been universally adopted. Under the ITSFEA, controlling persons may be subject to treble damages for "reckless disregard" of the fact that subordinates may engage

in violations, and for the failure to take appropriate steps to prevent such conduct. The failure to maintain an effective insider trading compliance program arguably could be evidence of "reckless disregard" under the statute. Under the federal sentencing guidelines, companies can reduce their "culpability score" for employees' insider trading by having an effective compliance program in place. Finally, the U.S. Department of Justice has indicated that the operation of effective compliance programs will impact its decision to prosecute firms for the actions of their employees.

The terms of insider trading policies vary considerably, however, and the manner in which companies administer their programs varies even more. Accordingly, before going into the specifics of how a program might be updated in response to recent events and the SEC Cybersecurity Guidance, it is useful to consider the purposes that these programs aim to serve. Attention to these "first principles" will inform many of the decisions that should be considered in implementing and updating a company's insider trading policies and procedures.

Insider trading compliance programs serve three main purposes:

- **Protecting the Company and Other Control Persons.** The last thing any public company and its officers and directors need is an insider trading investigation. At a minimum, these investigations require companies to produce extensive corporate records demonstrating what information was available, to whom and when. Arguments could also arise that corporate officers, and perhaps the company itself, are liable as "control persons" for illegal employee trading. The establishment, maintenance and enforcement of an effective insider trading compliance program should make it less likely that a company's insiders will engage in illegal activity. It should also mitigate exposure for the company and the distractions and expense of an investigation, in the event there is a bad actor.
- **Protecting the Company's Workforce.** Insider trading compliance programs also protect the company's directors, officers and other employees from becoming embroiled in the costly and distracting legal and reputational nightmare of defending against allegations of "insider trading." An officer seeking to sell some shares as part of her financial planning wants comfort that, if she does so, her actions will not become the subject of scrutiny. Consider, for example, the appearance of improper trading if her sale is followed by the company announcing disappointing news and a decline in the share price. As another example, if a company's policies and reminders encourage an officer, director or employee to protect material non-public information ("MNPI") from family members, a costly and embarrassing investigation triggered by a family member's trading could be avoided.
- **Protecting the Company's Reputation.** Allegations of insider trading against an employee, officer or director may cause significant reputational harm to a public company. Defending against this reputational damage may be expensive for the company and distracting for its workforce.

2. CONFIRM THAT MANAGEMENT AND THE BOARD ARE ALIGNED ON THE PHILOSOPHY BEHIND YOUR PROGRAM

Public companies face many choices in designing their insider trading compliance programs. These choices should be informed by balancing the risks that the company and its officers face from insider trading by company personnel against the costs of imposing an overly-restrictive policy. A highly restrictive policy may reduce the risk of the company and its managers facing an insider trading investigation, but there are costs to such an approach. At the extreme, the company's ability to use its equity securities in incentive compensation programs may be compromised if employees believe that they will not be able to sell those securities to meet their financial needs. In more pragmatic terms, an overly-restrictive program may be difficult to administer on a day-to-day basis, and may result in a pattern of non-compliance.

The company's culture may also come into play in designing and operating its insider trading compliance program. Some companies tend to impose more restrictions on any activities that could subject the company to legal liabilities,

with the added benefit of helping employees avoid difficult situations. Other companies take a more "hands-off" approach, restricting the activities of employees only when dictated by compelling needs of the company.

Whenever the company considers changes in its insider trading compliance program, it is important to ensure that the board and management are aligned on the purposes and philosophy embodied in the program.

3. ENSURE THAT YOUR INSIDER TRADING COMPLIANCE POLICY IS UP TO DATE AND FOLLOWS BEST PRACTICES

Before considering the appropriateness of updates to a company's insider trading compliance policy to address cybersecurity matters, it is useful to review some key operational elements employed by most policies. Most insider trading compliance policies:

- Prohibit trading or tipping by directors, officers and other employees (along with their respective family and household members) in possession of MNPI;
- Impose "window" restrictions around quarterly earnings announcements, so that certain individuals may trade only during limited periods of time each quarter;
- Require directors and senior officers privy to sensitive information to "pre-clear" their transactions;
- Provide that various types of purchases and sales by insiders will be exempt from these restrictions; and
- Allow the company to impose special trading blackouts in appropriate circumstances (e.g., a team working on a material acquisition or that has become aware of a material event).

With those key elements in mind, you should address the following points.

- **Consider whether cybersecurity incidents should be included among examples of events that may be material.**

Insider trading compliance policies uniformly prohibit trading while an employee, officer or director is in possession of any MNPI about the company. To assist individuals in their understanding of what constitutes MNPI, policies typically include a list illustrating the types of information that are likely to be considered "material." Some of these examples are applicable to all public companies (e.g., the company's quarterly results varying significantly from previous guidance or an impending change in senior management), while other examples should be tailored to risks specific to the company and its industry.

In view of the SEC Cybersecurity Guidance, we recommend that all public companies consider their risk profile, including with respect to cybersecurity, and update their list of examples of MNPI to reflect their current situation. Rather than simply listing "a material cybersecurity incident," consider whether the examples listed in your policy appropriately address the broader set of similar events your business might encounter. In addition to the company's technology infrastructure, consider risks to its facilities or fleet. Consider other types of events that could disrupt the company's operations. The following language, for example, would cover cybersecurity incidents, as well as a broader range of events – "a significant disruption in the company's operations or loss, potential loss, breach or unauthorized access of its property or assets, including its facilities and information technology infrastructure."

Companies should consider whether this type of list of examples of MNPI will be useful for its workforce, and any such list must be carefully tailored to include the types of information that are most important to the company. A policy that includes this type of list should state clearly that the examples are provided solely for illustration purposes and that they are not a complete list of types of events that might be material. Policies often remind employees that they have the

responsibility for being certain that they do not have MNPI when they enter into transactions and that they should consult supervisors or compliance personnel with any questions.

- **Confirm that the Company has an effective mechanism for imposing special blackouts.**

As described above, most insider trading compliance policies include provisions under which the company reserves the right to impose a trading blackout at any time, on any group of employees or officers (referred to as a "special blackout"). In the SEC Cybersecurity Guidance, the SEC focuses on the period when a company is investigating the underlying facts and assessing the materiality of a significant cybersecurity incident, prior to the time that it publicly discloses the incident. The SEC emphasizes that companies should consider whether and when it may be appropriate to implement a special blackout in this period.

In view of this guidance from the SEC, public companies should ensure that their insider trading compliance policies include appropriate provisions permitting them to impose special blackouts. Beyond including such a measure in the policy, each company should consider how it would identify employees who should be covered and how it would communicate with them, in an urgent situation. It may also be useful to consider, in advance, the types of transactions that might be exempt from a special blackout.

- **Consider whether other updates of your insider trading compliance policy might be appropriate.**

As companies experience changes in the way they do business, the composition of their workforces and their channels of public communication, it is useful for them to review and refresh their insider trading compliance policies. As you consider amendments to your policy relating to cybersecurity matters, the following are a few subjects that may also be worthy of consideration:

  - **Windows.** Is the timing for opening and closing the quarterly window in connection with earnings still consistent with the timing of financial information becoming available internally? For example, has the company implemented a new internal reporting system that provides better visibility into its quarterly results earlier in the quarter? Has the list of insiders who have regular access to financial information changed?
  - **Trading groups.** Are you comfortable with how employees, officers and directors are categorized between the group subject to pre-clearance and windows, the group subject to windows but no pre-clearance and the group restricted only when in possession of MNPI? For example, have you added personnel to your legal, finance, accounting, IR or IT functions that are privy to information that historically had only been available to officers who are subject to pre-clearance?
  - **Pre-clearance.** Does your policy reflect actual practice for obtaining pre-clearance and is responsibility for pre-clearance in the right hands? For example, should the company consider a committee approach to pre-clearance instead of designating one individual? What documentation and recordkeeping requirements are imposed for pre-clearance requests?
  - **New means of communications, security ownership or financial instruments.** Have there been developments in channels of communications or types of security ownership and financial instruments that should be expressly referenced in the policy? For example, does the policy adequately address the interplay between consumer engagement through the internet and social media channels, on the one hand, and unauthorized disclosure of MNPI and "tipping," on the other hand?
  - **Relationships with Third Parties.** Insider trading compliance policies typically touch other companies in two respects. First, company employees should be prohibited from trading on the basis of MNPI relating to other public companies that they obtain during the course of their work for the company. Second, policies often contain

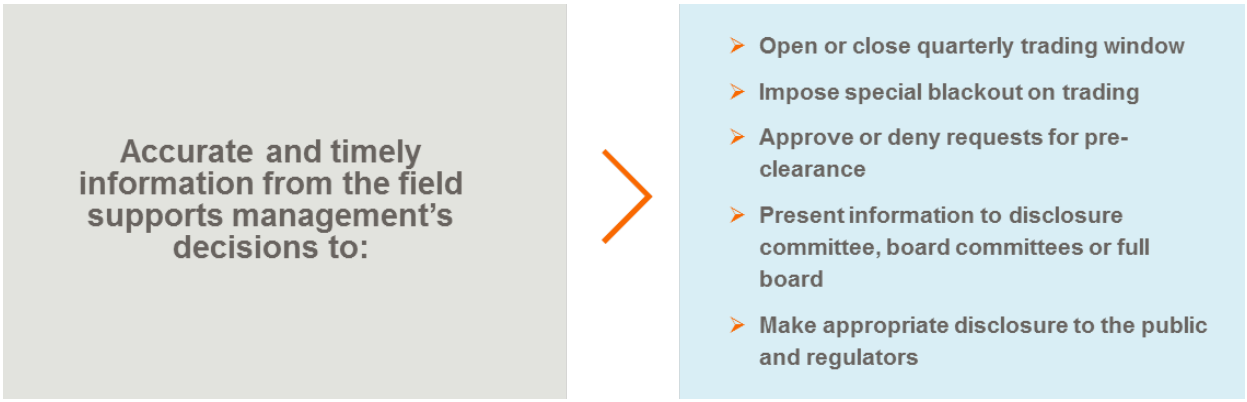
provisions calling on company employees to arrange for agreements with third party vendors, consultants and contractors, prohibiting these third parties from trading in company securities or disclosing MNPI. In view of new approaches to collaboration and the increased sharing of information with people outside of the company, the company may wish to consider its coverage of such third parties.

— **Recurring questions**. Whenever a company updates its policy, it should consider the types of recurring questions asked by employees, officers and directors. Addressing these issues in the policy should provide clarity for the workforce, improve consistency and reduce the burden of administering the program.

4. REVIEW AND UPDATE PROCESSES AND PROCEDURES FOR A CUSTOMIZED APPROACH TO POLICY ADMINISTRATION

Drafting a robust insider trading compliance policy is the easy part. The more significant challenge is ensuring that the company's processes and procedures relating to the flow of information and the administration of the policy are both effective and practical. With no "one size fits all" approach, it is important to work together with internal stakeholders and outside advisors to develop and implement customized processes and procedures that work for your company.

- **Information Flow.** It is critical that a company have effective disclosure controls for material events, including relating to cyber and data privacy matters. Companies must design reliable processes through which information will flow "from the field" to officers responsible for public disclosure and insider trading compliance, as well as processes through which headquarters personnel may pull information from the field. Among other things, proper flows of information enable the company to impose "special blackouts" when appropriate, as described above.



- **Coordination between public disclosure and insider trading compliance functions**. Given the increased focus on the accuracy and completeness of public disclosure related to cybersecurity, and the impact of information about cybersecurity on insiders' securities transactions, it is critically important to have effective coordination between those responsible for the company's public disclosure and its insider trading compliance program. Although it is appropriate for companies to use different "triggers" for denying pre-clearance of insiders' transactions, imposing special blackouts on groups of employees and making disclosure of an event to the public, decisions on these matters should be made on the basis of consistent information and legal analyses.

- **Pre-Clearance Officer or Committee.** Since there is no "check the box" guide to determining if an event such as a cybersecurity incident is "material" or disclosable, with the availability of information often evolving over time, even with the most systemized insider trading compliance program there will be pressure on people administering the policy to call the "balls and strikes" correctly. Companies should consider whether decisions to open or close windows, to pre-clear transactions or to impose special blackouts should rest with one individual (e.g., a senior legal officer) or instead with a small committee (e.g., a committee composed of legal, finance and compliance officers). We

believe there will be a trend toward more companies adopting the committee approach, thereby relieving a single individual from the responsibility (and scrutiny) of such decisions. There is no need for committees to meet in person or even confer by telephone, as electronic messages may allow them to work efficiently.

- **Basis of Granting Pre-Clearance.** Regardless of whether an individual officer or a committee will pass on requests for pre-clearance, it will be useful for the company to provide guidance regarding the standard and degree of conservatism to be employed in making the pre-clearance decision. Should only the existence of currently material information result in a denial, or should clearance also be denied if there is a real concern that information currently known could develop into MNPI? This is another example of a decision on which the board and senior management should be aligned, based on their approach to risk.
- **Administrative Nuts and Bolts.** Diligent day-to-day attention to the administration of the policy is important for its effectiveness, and operational matters should not be overlooked. Among other things, you should work with advisors to address the following points:
  - Establish processes for adding and removing individuals from pre-clearance and window groups, as well as for periodically confirming that the approach to classification is appropriate
  - Craft succinct communications for the opening and closing of windows, expected trading calendars, reminders, special blackouts etc.
  - Consider whether the company should obtain periodic certifications of compliance from employees, officers and directors, as well as certifications when an insider trades within a window or requests pre-clearance
  - Ensure that the company has proper recordkeeping for its insider trading compliance program, and consider what the records would show if the company were required to produce its records in an enforcement proceeding
  - Consider whether there are metrics that suggest insiders either are or are not complying with the company's policy. Do the numbers of inquiries about the policy or requests for pre-clearance suggest that insiders are complying with the policy?
- **Awareness and Training.** "Tone at the top" is an important component of any area of compliance and can be reinforced with a thoughtful approach to awareness and training. Consider how information is most effectively communicated through all levels of your organization and design procedures to disseminate information regarding your insider trading program and the importance of compliance. This includes considerations such as where the policy is made available, the frequency and content of communications about the policy and training programs on compliance. It is often helpful to view these items through the eyes of your least-sophisticated employee.
- While expediency is important, given the importance of establishing a program with policies and procedures that can and will be adhered to, we encourage those responsible for their program to undertake a methodical review of their insider trading compliance policy and program with the consultation of knowledgeable advisors. Please reach out to any of the King & Spalding attorneys listed herein if we can help.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,000 lawyers in 20 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to under- standing the business and culture of its clients.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered “Attorney Advertising.”

ABU DHABI	CHICAGO	HOUSTON	NEW YORK	SILICON VALLEY
ATLANTA	DUBAI	LONDON	PARIS	SINGAPORE
AUSTIN	FRANKFURT	LOS ANGELES	RIYADH	TOKYO
CHARLOTTE	GENEVA	MOSCOW	SAN FRANCISCO	WASHINGTON, D.C.