PRESENTATION

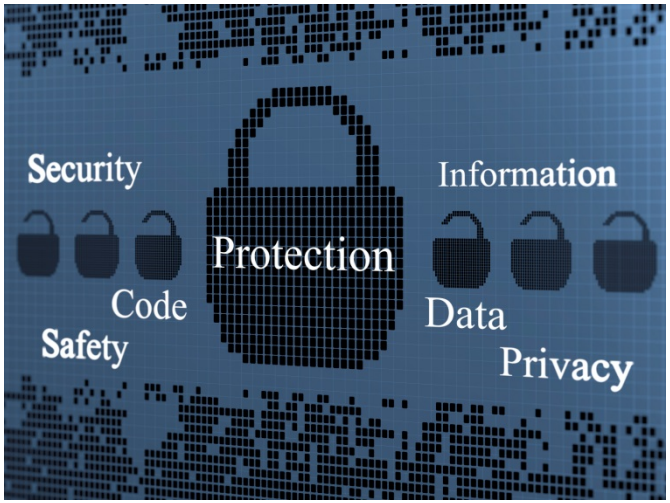
Cybersecurity: What Broker-Dealers, Investment Advisers, Management, and Compliance Need to Know

BAKER DONELSON

EXPAND YOUR EXPECTATIONS℠

Why Are We Here?

- SEC and FINRA Examinations
- Enforcement Activities
- Litigation
- Customer Inquiries/ Concerns



What is Cybersecurity?

- The Regulators take a broad view and define cybersecurity as the protection of investor and firm information from compromise through the use—in whole or in part—of electronic digital media, (e.g., computers, mobile devices or Internet protocol-based telephony systems).
- "Compromise" refers to a loss of data confidentiality, integrity or availability.

See, e.g., FINRA Report on Cyber Security Practices (Feb. 2015).

Cybersecurity Threats:

- The SEC recently examined 57 registered broker-dealers and 49 registered investment advisers to better understand how firms address the legal, regulatory, and compliance issues associated with cybersecurity. The Survey found that 88% of broker-dealers and 74% of advisers have experienced cyber attacks, either directly or through a vendor.

- Top 3 Threats identified by FINRA in both 2011 and 2014:
  - hackers penetrating firm systems;
  - insiders compromising firm or client data; and
  - operational risks.

Common Cyber-Vulnerabilities

- Hackers
- Poor Controls- Change Management Failures
- Data Loss – Laptops and especially PDAs
- Disaster Recovery & Business Continuity Plans
- Rogue Employees
- Phishing Scams

and of course. . . there is always

- Stupidity

Summary of Firm Responses Identifying Top Three Threats

	2014 Sweep Results (% of respondents ranking threat as 1st, 2nd or 3rd)			2011 Survey Results (% of respondents ranking threat as 1st, 2nd or 3rd)		
	1st	2nd	3rd	1st	2nd	3rd
Cyber risk of hackers penetrating systems for the purpose of account manipulation, defacement or data destruction, for example	33	28	11	38	33	19
Operational risk associated with environmental problems (*e.g.*, power failures) or natural disasters (*e.g.*, earthquakes, hurricanes)	22	17	17	31	16	29
Insider risk of employees or other authorized users abusing their access by harvesting sensitive information or otherwise manipulating the system or data undetected	22	11	33	24	35	22
Insider risk of employees or other authorized users placing time bombs or other destructive activities	0	11	0	0	4	5
Cyber risk of non-nation states or terrorist groups penetrating systems, for example, for the purpose of wreaking havoc	0	6	6	0	4	5
Cyber risk of nation states penetrating systems, for example, for the purpose of espionage	0	6	6	0	2	5
Cyber risk of competitors penetrating systems, for example, for the purpose of corporate espionage	0	0	0	0	2	4

What Not to Do

Where to Start?

- Know What Information You Have and Know Where It Is
- Examination of the Potential Threats and Vulnerabilities
- Understand Existing Controls & Missing Controls
  - Administrative Controls
  - Physical Controls
  - Technical Controls

What Should You Do?

- Follow the Guidance from FINRA and the SEC:
  - Make sure you have cybersecurity governance and risk assessment processes appropriate for your business.
  - Make sure you have basic controls to prevent unauthorized access to systems or information.
  - Make sure you have adequate data loss prevention controls.
  - Make sure you are adequately managing your vendors.
  - Make sure you are doing adequate training.
  - Make sure incidence response plans are developed to address possible future cybersecurity events.

1. Make sure you have cybersecurity governance and risk assessment processes appropriate for your business.

At a minimum, you should make sure you do the following:

- Have firm policies and procedures related to protection of broker-dealer customer and/or investment adviser client records and information that are tailored to your business and the specific threats and risks that are most important or relevant to you. Some key areas that SEC has mentioned it will check for are:
  - Policies on patch management practices
  - Policies on penetration testing, whether conducted by or on behalf of the firm,
  - Policies on the firm's vulnerability scans
- Make sure your Board, and Senior Management, have been informed regarding: cyber-related risks; cybersecurity incident response planning; actual cybersecurity incidents; and cybersecurity-related matters involving vendors and have Board minutes and briefing materials to prove it.
- Have a Chief Information Security Officer ("CISO") or equivalent position, and other employees responsible for cybersecurity matters.
- Make sure that you have identified the positions and departments responsible for cybersecurity-related matters and that this is documented in the firm's organizational structure and on an org chart so that regulators can see how they fit into the organizational hierarchy.
- You need to be doing periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business and compliance consequences, if applicable, and have a record of the assessments, any resulting findings and the responsive remediation efforts taken.

Case study:

- In one instance where FINRA took enforcement action, hackers attacked a firm's server to obtain confidential customer information of more than 200,000 customers, including names, account numbers, SS numbers, addresses and dates of birth. The firm stored the data on a computer with an Internet connection and did not encrypt the information. The firm only became aware of the breach when hackers attempted to extort money from the firm despite that the breaches were visible on the firm's Web server logs.
- The case illustrates governance failures in several respects. Most broadly, the firm failed to implement adequate safeguards to protect customer information. More specifically, the firm stored unencrypted confidential customer data on a database connected to the Internet without effective password protection. Although the firm performed penetration testing, it did not include an asset with sensitive customer information as part of that test. In addition, the firm did not establish procedures to review the Web server logs that would have revealed the theft of data. And, the firm did not respond to an earlier auditor recommendation that it acquire an intrusion detection system. Finally, the firm also failed to have written procedures in place for its information security program designed to protect confidential customer information.

2. Make sure you have basic controls to prevent unauthorized access to systems or information.

At a minimum make sure you do the following:

- Have firm policies and procedures regarding access by unauthorized persons to firm network resources and devices and user access restrictions (e.g., access control policy, acceptable use policy, administrative management of systems, and corporate information security policy), including those addressing the following:
- Establishing employee access rights, including the employee's role or group membership and reviewing employee access rights and restrictions
- Updating or terminating access rights based on personnel or system changes
- Any management approval required for changes to access rights or controls.
- Log-in attempts, log-in failures, lockouts, and unlocks or resets
- Devices used to access the firm's system externally (i.e., firm-issued and personal devices), including those addressing the encryption of such devices and the firm's ability to remotely monitor, track, and deactivate remote devices.
- Verification of the authenticity of customer requests to transfer funds.
- Regarding system notifications to users, including employees and customers, of appropriate usage obligations when logging into the firm's system (e.g., log-on banners, warning messages, or acceptable use notifications.

2. Make sure you have basic controls to prevent unauthorized access to systems or information (con't).

- Make sure you can document the implementation of these firm policies and procedures related to employee access rights and controls, such documentation evidencing the tracking of employee access rights, changes to those access rights, and any manager approvals for those changes;
- Use multi-factor authentication for employee and customer access as well as documentation evidencing implementation of any related policies and procedures and information on systems or applications for which the firm does not use multi-factor authentication.
- Keep track of instances in which system users, including employees, customers, and vendors, received entitlements or access to firm data, systems, or reports in contravention of the firm's policies or practices or without required authorization as well as information related to any remediation efforts undertaken in response.
- Keep documentation on review of access rights and restriction and on any internal audits done that covered access rights and controls.

Case Study:

- The SEC recently commenced a settled enforcement action against an investment adviser, R.T. Jones Capital Equities Management, Inc., for cybersecurity matters. From at least September 2009 through July 2013, R.T. Jones stored sensitive personally identifiable information, or PII, of clients and other persons on its third party-hosted web server without adopting written policies and procedures regarding the security, confidentiality, and protection from unauthorized access. In July 2013, the firm's web server was attacked by an unauthorized, unknown intruder, who gained access rights and copy rights to the data on the server. As a result of the attack, the PII of more than 100,000 individuals, including thousands of R.T. Jones's clients, was rendered vulnerable to theft. After the breach, R.T. Jones retained a cybersecurity firm to confirm the attack and assess and trace the origin of the breach. They hired another firm to review the initial report and conduct another assessment. R.T. Jones also provided notice of the breach to all of the individuals whose PII may have been compromised and offered them free identity monitoring through a third-party provider. The SEC asserted that R.T. Jones failed to adopt written policies and procedures reasonably designed to protect customer records and information, in violation of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)). R.T. Jones is paying a $75,000 civil penalty in settlement of this matter.

3. Make sure you have adequate data loss prevention controls.

At a minimum, make sure you do the following:

- Have firm policies and procedures related to enterprise data loss prevention and information related to the following:
- Data mapping, with particular emphasis on understanding information ownership and how the firm documents or evidences personally identifiable information (“PII”).
- The systems, utilities, and tools used to prevent, detect, and monitor data loss as it relates to PII and access to customer accounts, including a description of the functions and source of these resources.
- Have firm policies related to data classification, including: information regarding the types of data classification; the risk level (e.g., low, medium, or high) associated with each data classification; the factors considered when classifying data; and how the factors and risks are considered when the firm makes data classification determinations.
- Have firm policies and procedures related to monitoring exfiltration and unauthorized distribution of sensitive information outside of the firm through various distribution channels (e.g., email, physical media, hard copy, or web-based file transfer programs).
- Make sure you can document implementation of these policies.

4. Make sure you are adequately managing your vendors.

At a minimum, make sure you do the following:

- Have policies and procedures related to third-party vendors, such as those addressing the following:
  - Due diligence with regard to vendor selection.
  - Ongoing due diligence with respect to selected vendors.
  - Contracts, agreements, and the related approval process.
  - Supervision, monitoring, tracking, and access control.
  - Any risk assessments, risk management, and performance measurements and reports required of vendors.
- Keep documentation and records regarding third-party vendors with access to the firm's network or data, including those that facilitate the mitigation of cybersecurity risks by means related to access controls, data loss prevention, and management of PII, including the services provided and contractual terms related to accessing firm networks or data.
- Have a written contingency plan with your vendors concerning issues that might put the vendor out of business, put them in in financial difficulty or that might make it difficult for them to continue working with you (for instance, conflicts of interest, bankruptcy, etc.).
- Establish and implement procedures to terminate vendor access to firm systems immediately upon contract termination
- Prepare and keep sample documents or notices required of third-party vendors, such as those required prior to any significant changes to the third-party vendors' systems, components, or services that could potentially have security impacts to the firm and the firm's data containing PII.

Case Study

- At one firm, the Purchasing department leads the vendor selection process with a steering committee, including members from six due diligence teams (Technical Architecture, IT Control Risk Assessment, Financial, Legal, Compliance and Business Continuity Management). To get a vendor approved, a business unit must submit a purchase request form to Purchasing to initiate the process (e.g., contract, request for proposal, request for information). The form includes 20 to 30 questions that help Purchasing decide the level of inherent risk and which due diligence teams should be involved in vetting the potential vendors. When the IT Control Risk Assessment team is involved, it uses questionnaires focused on the type of data or potential risk involved in the vendor process. These questionnaires are sent to each potential vendor for completion. Where customer PII would be sent off-site or a cloud vendor is involved with PII, the firm uses the most detailed list of questions. In addition, where customer PII or other highly sensitive data is involved, an independent attestation is required. The IT Control Risk Assessment team scores firm responses from 0 (low risk) to 100 (high risk). Should the business desire to accept a vendor with a residual high-risk score, approval from a senior vice president would be required. All contracts include standardized language for 28 identified areas, including controls, the right to audit, confidentiality and security, regulatory compliance, insurance coverage, business continuity planning, subcontracting, encrypting, incident reporting, storage of data and an exit strategy.

5. Make sure you are doing adequate training.

Given that many data breaches result from unintentional employee actions, regulators want to make sure you are doing training that is tailored to employees' specific job functions and which is designed to encourage responsible employee and vendor behavior. Accordingly, make sure you do the following:

- Provide appropriate training to employees on information security and risks and keep documentation regarding the training, including the training method (e.g., in person, computer-based learning, or email alerts); dates, topics, and groups of participating employees; and any written guidance or materials provided. Such training should include delivering interactive training materials and encourage audience participation. Training should be done periodically on training update cycles. Some basic topics that should be covered for everyone are:
  - How to deal with a misplaced laptop or PDA
  - When and how to communicate with clients and third parties securely
  - Prohibitions on the use of unsecured internet connection to access client data
  - Opening messages or downloading attachments from an unknown source
- Provide appropriate training to vendors and keep documentation regarding the training provided.

Case Study

- An example of an effective ad hoc training program is a firm's response to a phishing attack. In this instance, a hacker was able to gain access to a client's personal email. The hacker then portrayed himself as the client of the firm and sent written instructions to wire transfer funds to an offshore bank account. Since the amount of the transfer was not unusual and the client frequently wired transferred funds, neither the registered representative nor branch office staff called the client to confirm the transaction. Only after the funds were sent, did the firm discover that the source of the transfer instructions was fraudulent. After completing the investigation, which revealed a lapse in firm procedures, the firm implemented new required verification of client instructions and rolled out a specific training requirement for all registered representatives and support staff. The firm provided the training materials and required branch management to host a meeting for all employees within their respective offices to ensure everyone was aware of the new requirements to verbally confirm all transfer instructions received.

6. Make sure incidence response plans are developed to address possible future cybersecurity events.

Make sure you do the following:

- Have policies and procedures regarding a business continuity of operations plan that address mitigation of the effects of a cybersecurity incident and/or recovery from such an incident, including policies regarding cybersecurity incident response and responsibility for losses associated with attacks or intrusions impacting clients.
- Have practices incorporating current threat intelligence to identify the most common incident types and attack vectors.
- Create containment and mitigation strategies for multiple incident types as well as eradication and recovery plans for systems and data.
- Conduct tests or exercises of your incident response plans and keep information regarding these tests, including the frequency of, and reports from, such testing and any responsive remediation efforts taken, if applicable.
- Document system-generated alerts related to data loss of sensitive information or confidential customer records and information, including any related findings and any responsive remediation efforts taken.

6. Make sure incidence response plans are developed to address possible future cybersecurity events (con't).

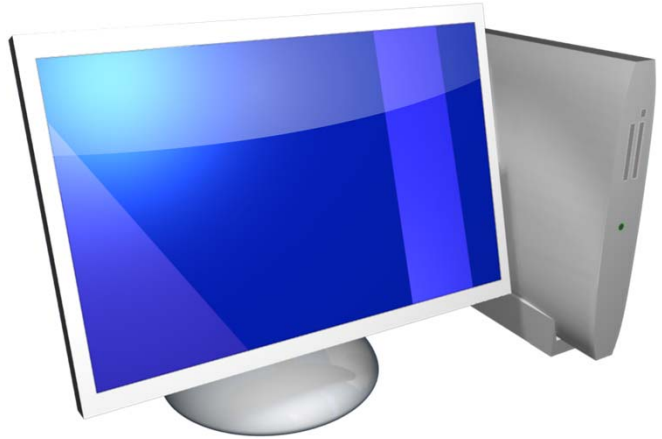
- Document incidents of unauthorized internal or external distributions of PII, including the date of the incidents, discovery process, escalation, and any responsive remediation efforts taken.
- Document the amount of actual customer losses associated with cyber incidents, as well as information on the following:
  - The amount of customer losses reimbursed by the firm.
  - Whether the firm had cybersecurity insurance coverage, including the types of incidents the insurance covered.
  - Whether any insurance claims related to cyber events were filed.
  - The amount of cyber-related losses recovered pursuant to the firm's cybersecurity insurance coverage.
- Implement measures to maintain client confidence, including:
  - the provision of credit monitoring for individuals whose personal information has been compromised; and
  - the reimbursement to customers for financial losses incurred.

Case Study

- One firm reviewed has a dedicated Computer Security Incident Response Team. One of the team's first steps in developing the firm's incident response plans was to determine the most likely types of incidents to which the firm would need to respond. The firm then established a leader for the incident response process and an internal leader for each type of incident as well. The incident response process also includes management personnel (e.g., representatives from Legal & Compliance, Human Resources, Corporate Communication [internal and external] and IT) to assist in the response effort. In addition, the CSIRT identified the role of each party and the workflow of the response steps. Involved parties include outside sources such as forensic experts, outside counsel and vendors that would handle call center and credit monitoring functions, if necessary. In developing its incident response plan, the firm furthered its understanding of the requirements for data preservation to allow for thorough forensic analysis; established a baseline for "normal" activity so that legitimate issues can be differentiated from false positives; and identified useful external resources. The firm regularly runs exercises that help it to identify any gaps in its plans and which also serve as a training tool. The firm updates its plans on an ongoing basis to incorporate lessons learned from the exercises, as well as identified new threats.

When Something Goes Wrong: Breach Incident Response

- Identification of Team
- Identification of Vendors
- Understanding of State and Federal laws and DEADLINES
- Understanding Steps to take
- Law Enforcement contacts
- Regulators to contact
- Prepared with Credit Monitoring



E.g., Customer Notification (In Tennessee):

Tennessee	Legislation	Tenn. Code Ann. § 47-18-2107
	Entities Covered	"Any information holder shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data"
	Data Covered	"an individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when either the name or the data elements are not encrypted: (i) Social security number; (ii) Driver license number; or (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account."
	Def'n of Breach	"unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the information holder."
	Who to Notify	"any resident of Tennessee whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."
	Means of Notice	"by one (1) of the following methods: (1) Written notice; (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code; or (3) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the information holder does not have sufficient contact information. Substitute notice shall consist of all of the following: (A) E-mail notice when the information holder has an e-mail address for the subject persons; (B) Conspicuous posting of the notice on the information holder's Internet website page, if the information holder maintains such website page; or (C) Notification to major statewide media."
	Timing of Notice	"in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (d), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."
	Exemptions	"an information holder that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system."
	Penalties	"Any customer of an information holder that is a person or business entity, but that is not an agency of the state or any political subdivision of the state, and who is injured by a violation of this section may institute a civil action to recover damages and to enjoin the person or business entity from further action in violation of this section."
	Third Parties	"Any information holder that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."
	Effective Date	7/1/2005

Cybersecurity Litigation:

- Courts have historically dismissed cases alleging liability for data breaches where the Plaintiff has not suffered an injury in fact. However, several courts have held that the threat of future harm or increased risk of future harm satisfies the injury in fact requirement. *See, e.g., Pisciotta v. Old National Bankcorp*, 499 F.3d 629 (7th Cir. 2007).

- Class Action Theories:
  - Breach of implied covenant of good faith and fair dealing,
  - Breach of contract, breach of implied contract,
  - Negligence, negligence per se
  - Breach of fiduciary duty, and
  - Unjust enrichment

Cyber Coverage – Insurance.

- FINRA's Survey found that Firms identified three sources of cyber insurance coverage:
  1) a standalone policy specifically underwritten by the insurance carrier to provide the firm with cyber insurance;
  2) obtaining cybersecurity liability riders in connection with a firm's existing insurance policies (i.e., fidelity bond, errors and omissions policies); and
  3) relying on a firm's existing insurance policies (i.e., errors and omissions) that included some, but limited, coverage to cyber-related incidents.
- The standalone policies firms purchased typically cover data breaches, remediation cost reimbursement limits to respond to the breaches, and coverage for regulatory and legal fines and penalties.

Cyber Coverage – Insurance (Cont'd).

- Among the firms FINRA reviewed:
  - 61 percent purchased standalone cybersecurity insurance;
  - 11 percent purchased a cybersecurity rider with their fidelity bond; and
  - 28 percent did not rely on any type of cybersecurity insurance at the time of the sweep.
- Typically, large firms purchased standalone policies, where they had the ability to customize the types and amount of coverage based on their risk appetite.
- However, smaller and mid-size firms with limited cybersecurity risk typically purchased cybersecurity riders in connection with existing fidelity bond policies.
- None of the firms with either type of coverage made cyber insurance-related claims to recover losses.
- Firms also commented that the market for cyber insurance is relatively new and evolving rapidly. There is now greater diversity of coverage available and at more affordable rates, in some cases.

Cyber Coverage – Insurance (Cont'd).

- As a result, FINRA urges firms to monitor developments in the cyber insurance market and to evaluate what role, if any, it can play in a firm's efforts to mitigate cybersecurity risks and absorb the financial ramifications of a cyber-related event.
- Specifically, Firms should evaluate the utility of cyber insurance as a way to transfer some risk as part of their risk management processes. Effective practices include:
  - for firms that have cybersecurity coverage, conducting a periodic analysis of the adequacy of the coverage provided in connection with the firm's risk assessment process to determine if the policy and its coverage align with the firm's risk assessment and ability to bear losses; and
  - for firms that do not have cyber insurance, evaluating the cyber insurance market to determine if coverage is available that would enhance the firm's ability to manage the financial impact of cybersecurity events.
- Thus, Firms should assess:
  - Do existing insurance policies cover any aspects of cybersecurity events?
  - Which events are insurable?
  - Do the firm's risk management approaches adequately cover the financial risks associated with cybersecurity events?
  - What coverage will a new or enhanced cyber insurance policy provide and what will it cost?

Questions?

Lori Patterson
Baker, Donelson, Bearman, Caldwell & Berkowitz, PC
First Tennessee Building
165 Madison Avenue, Suite 2000
Memphis, TN 38103
Direct: 901.577.8241
Fax: 901.577.0768
Email: lpatterson@bakerdonelson.com

References:

- FINRA Report on Cyber Security Practices (Feb. 2015) available at: https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

- SEC 2015 Cyber Security Examination Sweep Summary available at: https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf

- SEC's OCIE 2015 Cybersecurity Examination Initiative available at: https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

- SEC's OCIE Cybersecurity Initiative (2014) available at: https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf

PRESENTATION

Fall Compliance Roundtable
FINRA Research Analyst Rules

Thursday, October 29, 2015

BAKER DONELSON

EXPAND YOUR EXPECTATIONS℠

Evolution of Research Analyst Rules

- **Sarbanes-Oxley Act**
- **Initial Rules adopted in 2002**
- **Additional rules adopted in 2003, 2005, and 2006**
- **Rule amendments in 2012**
- **Amendments to equity analyst rule and new rules for debt analysts become effective December 24, 2015 – Merry Christmas!**

FINRA Rules 2241 and 2242 – An Overview

- Identifying and Managing Conflicts of Interest
  - Principles-based Policies and Procedures
  - Specific Requirements of Policies and Procedures
- Content and Disclosure in Reports
  - Specific Requirements of Policies and Procedures
  - Ratings Requirements
  - Financial Interest & Compensation
  - Other Material Conflicts of Interest
- Public Appearances
- Distribution of Member Research Reports
- Distribution of Third-Party Research Reports
- Exemptions

Some Key Terms

- **Research Analyst**
  - associated person
  - primarily responsible for preparation of research report or
  - reports to a research analyst
- **Research Report**
  - written communication
  - analysis of security or issuer or industry
  - provides information upon which to base an investment decision
  - certain exclusions
    - excludes general commentaries
    - excludes communications to less than 15 persons
    - excludes statutory prospectuses and PPMs

Some Key Terms (continued)

- **Investment Banking Services**
  - underwriting
  - participation in a selling group
  - financial adviser in a merger or acquisition
  - providing venture capital or equity lines of credit
  - placement agent
  - otherwise acting in furtherance of a private or public offering

Principles Based Portion of Rule

- Policies to ***identify*** and ***effectively manage*** conflicts of interest related to:
  - preparation, content and distribution of research reports
  - public appearances by research analysts
  - interaction between research analysts and ***others***
- Policies must:
  - promote objective and reliable research
  - reflect the truly held opinions of research analysts
  - prevent the use of reports to manipulate the market
  - not favor the interests of the member or customers

Principles-Based Rule Intersects with Specific Restrictions

- Specifically, policies must:
  - prohibit prepublication review or approval by certain parties
  - restrict input into reports by certain parties
  - prohibit certain parties from supervising research personnel
  - limit determination of budget to senior management, excluding certain parties
  - prohibit compensation based on investment banking services
  - annual review and approval of compensation by committee that reports to the board or a senior executive officer if no board
  - compensation review must take into account certain factors
  - establish information barriers

Principles-Based Rule Intersects with Specific Restrictions (continued)

- Specifically, policies must:
  - prohibit retaliation against research analysts
  - (for equity only) define period during which the member must not publish reports and analysts must not make public appearances
  - restrict trading in securities covered by the analyst
  - prohibit promises of favorable research or a particular rating
  - restrict activities that can reasonably be expected to compromise their objectivity
  - prohibit investment banking personnel from directing an analyst to engage in marketing activities or any communications with a customer about an investment banking transaction
  - prohibit prepublication review of a report by a subject company

Content and Disclosure in Reports

- Policies must be reasonably designed to ***ensure*** that:
  - facts in reports are based on reliable information
  - any recommendation has a reasonable basis
  - reports include a clear explanation of any valuation method used
  - reports include a fair presentation of the risks that may impede achievement of the recommendation
- Each report must include the meaning of each rating used, the time horizon and any benchmarks on which a rating is based.
- Definition of each rating must be consistent with the plain meaning.
- Must include the percentage of companies assigned “buy” “hold” and “sell” categories and percentage of company which the member has provided investment banking services within past year

Content and Disclosure in Reports (continued)

- If the report contains a rating or price target, and the member has assigned a rating or price target for at least one year, then
  - (equity only) the report must include a line graph of the security's daily closing prices and ratings information
  - (debt only) the report must show each date on which a member has assigned a rating and the rating assigned
- Must disclose if the analyst or a member of the analyst's household has a financial interest in the securities of the subject company and the nature of such interest
- Must disclose if the analyst has received compensation based upon the member's investment banking revenues (debt only – or sales and trading or principal trading revenues)

Content and Disclosure in Reports (continued)

- Disclosures relating to compensation and interest in subject company by member or its affiliates:
  - managed or co-managed public offering in last 12 months
  - received compensation for investment banking services in last 12 months
  - expect to seek or receive compensation for investment banking services in next 3 months
  - received compensation for products or services other than investment banking services in the last 12 months
  - if the subject company has been a client over the last 12 months, and the type of services provided
  - (equity only) if ownership of subject company is 1% or more

Content and Disclosure in Reports (continued)

- Disclosures relating to compensation and interest in subject company by member or its affiliates:
  - (equity only) if the member was making a market in the securities at the time of the report
  - (debt only) if the member trades or may trade as principal in the debt securities that are the subject of the report
  - if the analyst received any compensation from the company during the past 12 months
  - ***any other material conflict of interest*** of the analyst or member that the analyst or any associated person of the member with the ability to influence the content of a research report knows or has reason to know

Content and Disclosure in Reports (continued)

- Disclosures must be presented on the front page of research reports or the front page must refer to where the disclosures are located
- All disclosures must be clear, comprehensive and prominent
- Must keep in mind additional disclosures required under FINRA and SEC rules

Disclosure in Public Appearances

- Public Appearance means any participation by an analyst where a recommendation is made in
  - a conference call, seminar, or other public speaking activity before 15 or more persons, or
  - an interview for radio, television or print media, or writing of a print media article
- Public Appearance doesn't include a password protected webinar, conference call or similar event with 15 or more existing customers, provided that all participants previously received the most current research report

Disclosures in Public Appearances

- Disclosures similar, but more abbreviated than report disclosures:
  - if the analyst or a member of the analyst's household has a financial interest in the securities of the subject company and the nature of such interest
  - (equity only) if ownership of subject company is 1% or more
  - if, to the extent the analyst knows or has reason to know, the member or any affiliate received any compensation from the subject company in the past 12 months
  - if the analyst received any compensation from the subject company in the past 12 months
  - if, to the extent the analyst knows or has reason to know, the subject company is or was during the past 12 months, a client
  - **any other material conflict of interest**

Distribution of Research Reports

- Policies must be reasonably designed to ensure that a report is not distributed selectively to trading personnel or a particular customer or class of customers in advance of other customers

Distribution of Third-Party Research Reports

- (equity only) A registered principal or supervisory analyst must review for compliance with FINRA rules
- May not distribute third-party research if the member knows or has reason to know such research is not objective or reliable
- Policies must be reasonably designed to ensure that any third-party research contains no untrue statement of material fact and is otherwise not false or misleading (no review required if the report is an independent third-party report)
- Must accompany any third-party research report with disclosure of any material conflict of interest
- Must ensure any third-party research report is clearly labelled as such

Exemptions

- Members with limited investment banking activity
  - relief only with respect to certain specific prohibitions
  - no relief from general policies and procedures or disclosures
- (debt only) Members with limited principal trading activity
  - relief only with respect to certain specific prohibitions
  - no relief from general policies and procedures or disclosures
- (debt only) Reports provided to institutional investors
  - Rule generally doesn't apply to reports distributed to QIBs and Institutional Accounts, subject to certain affirmations
  - Member not relieved from general policy requirements
  - Reports must prominently disclose the report is intended for institutional investors pursuant to the exemption

Questions?

Jackie Prester

Baker, Donelson, Bearman, Caldwell & Berkowitz, PC

First Tennessee Building

165 Madison Avenue, Suite 2000

Memphis, TN 38103

Direct: 901.577.8114

Fax: 901.577.0762

Email: jprester@bakerdonelson.com