CCO TASK SUPPORT

Please be sure to check your SmartRIA CCO portal to keep up with your monthly Compliance tasks.

Please contact the following for:

- **Task Related Questions:** Nancy Harry: nharry@thecomplianceresource.com
  Stacie Craddock: scraddock@thecomplianceresource.com
  Sara Sparks: ssparks@thecomplianceresource.com
- **Smart RIA Login & Portal Requests:** Sara Sparks: ssparks@thecomplianceresource.com
- **CRP Website & E-mail Communications:** Lindsay Rider: lrider@thecomplianceresource.com

CCO TOOLS INCLUDED THIS MONTH:

- **CCO Checklist** – Complete the attached CCO Checklist for the month of September 2022.

ATTENTION FIRMS: SEC HAS REG BI BACK IN FOCUS – DO YOU?

Last month, the U.S. Securities and Exchange Commission (SEC) published a Staff Bulletin providing guidance regarding conflicts of interest under broker-dealer Regulation Best Interest (Reg BI) and investment adviser fiduciary duty standards. The recent Bulletin, "*Standards of Conduct for Broker-Dealers and Investment Adviser Conflicts of Interest*," signals the continued focus on conduct standards and the sprawling interpretation of these standards. The Bulletin also reminds firms of their obligation — often beyond disclosure. The SEC does not want this to be merely a 'check-the-box' exercise, but a robust, ongoing process that is tailored to each conflict. The format of the Bulletin presents guidance in response to 13 questions posed by a hypothetical firm. The following themes are discussed below. **To read the entire SEC bulletin, CLICK HERE.** We highlight the themes below:

CONFLICTS OF INTEREST CAN TAKE MANY DIFFERENT FORMS

Conflicts can be consciously and/or unconsciously, according to the SEC. Similarly, compensation, revenue, or other benefits to the firm or financial professional can be financial or otherwise. For example, compensation based on assets gathered and/or products sold, or it can be tied to, or other rewards associated with quotas, bonuses, sales contests, or special awards. This can also include gifts, entertainment, meals, travel, and/or related benefits in connection with the financial professional's attendance at third-party sponsored trainings and conferences.

PERFORM PERIODIC REVIEWS

Annually, investment advisers are required to review the adequacy of such policies and procedures and the effectiveness of their implementation. The staff believes that identifying and addressing conflicts is not a "set it and forget it" exercise. Monitoring conflicts through an annual risk assessment exercise is recommended.

DISCLOSURE IS NOT ENOUGH

Disclosure of conflicts alone does not satisfy the obligation to act in a retail investor's best interest. Where such conflicts cannot be effectively addressed through mitigation, firms may need to determine whether to eliminate the conflict or refrain from providing advice or recommendations that are influenced by that conflict to avoid violating the obligation to act in a retail investor's best interest in light of the investor's objectives.

COMPENSATION / BENEFITS NEEDS TO COVER FIVE MAIN FACTS

When the conflict concerns compensation or other benefits, facts disclosed should, at a minimum, include:

- the **NATURE** and **EXTENT** of the conflict;
- the **INCENTIVES** created by the conflict and how the conflict affects or could affect the recommendation or advice provided to the retail investor;
- the **SOURCE(S) AND SCALE** of compensation for the firm and/or financial professional;
- how the firm and/or financial professional **is compensated for their recommendation;**
- or the nature and extent of **any costs or fees incurred, directly or indirectly, by the retail investor** as a result of the conflict.

FACTORS TO CONSIDER WHEN MITIGATING A CONFLICT

Several factors a firm should consider related to the nature and significance of the incentive, includes:

- Source of the firm's compensation,
- Whether or not it receives them directly from the retail investor;
- Extent to which a firm's revenues vary based on the type of account, products, services recommended;
- Whether or not the firm or its affiliates recommend or provide advice about proprietary products;
- Extent to which the firm uses incentives to encourage financial professionals to recommend or provide advice about accounts or investment products that are more profitable for the firm;
- Extent to which the compensation varies based on the investment product recommended;
- Nature of the payment structure for financial professionals (e.g., whether retrospective, the steepness of the increases between levels);
- Size or structure of the firm or if the firm's financial professionals are dually licensed or engage in activities outside of the firm; retail investor base; and the complexity of the security or investment strategy involving securities that are recommended.

DISCLOSURES SHOULD BE TAILORED

Disclosures should be specific to each conflict, in "plain English," and tailored to, among other things, firms' business models, compensation structures, and products offered at different firms. Stating that a firm "may" have a conflict when the conflict actually exists is not sufficiently specific to disclose the conflict adequately to retail investors.

CCO REVIEW: EMPLOYEES WORKING REMOTELY?

For firms allowing employees to office remotely, please review the checklist below to ensure the firm's information security programs are adequately assessed and address risks specific to working remotely.

REMOTE OFFICE

For some firms, the idea of remote officing continues. For these firms allowing employees to office remotely, proper policies and procedures need to be in place to appropriately oversee advisory activities. The SEC recommends that firms assess their information security programs to address risks specific to working remotely:

- remote access and the use of web-based applications;
- increased use of personally owned devices;
- changes in control over physical documents; and
- increased opportunities for phishing and social engineering.

In addition, please consider the following:

- ☐ **ACCESS RIGHTS.** Review firm personnel's access rights and controls. Firms may want to specifically consider whether they have applied principles of least privileged access, updated to reflect changed roles and responsibilities over the past few months. Firms may also want to consider whether existing logging is sufficient to capture privileged access to sensitive data and whether existing monitoring provides real-time, actionable alerts.

- ☐ **ENCRYPTION.** Use validated encryption techniques or other industry-recognized standards to protect communications and data at rest, including on personally owned devices.

- ☐ **PATCH MANAGEMENT.** Ensure remote access servers are secured and maintained as fully patched. Firms may want to consider whether they are effectively scanning for vulnerabilities and following patch management schedules and that any risk-rated framework for prioritizing vulnerabilities for remediation is appropriate to current operating conditions.

- ☐ **MULTIFACTOR AUTHENTICATION**. Ensure enhanced system access security, including by requiring the use of multifactor authentication.

- ☐ **THIRD-PARTY OVERSIGHT**. Review relevant contractual language or information security exhibits to verify third-party cybersecurity and their contractual rights to issue supplemental vendor security questionnaires. Firms may want to confirm that any open remediation items from prior due diligence exercises have been addressed and resolved.

- ☐ **TRAINING.** Provide supplemental training and reminders that address risks specific to working from home or new practices driven by working-from-home arrangements. These may include anti-phishing training, cautioning against the use of web-based applications to share information if unsecured, promoting the use of encryption, and reinforcing the importance of secure disposal of physical records at remote locations.

- ☐ **IDENTITY PROTECTION.** Firms should implement a policy and remind investors to contact them directly by telephone at a known and trusted number to report any suspicious activity. Firms are encouraged to review their wire transfer/disbursement policies and procedures with additional measures to validate the individual's identity, accuracy of information provided, and authorization to make the request. Firms may also want to consider whether any internal authorization requires multiple approvals and validation by telephone to a previously established, trusted number.