THIS MONTH IN COMPLIANCE
Review of Terminated IARs, SEC Commentary on FORM CRS Filings
Review of Third-Party Vendors

AUGUST COMPLIANCE TASKS

SMART RIA

Please be sure to check your SmartRIA CCO portal to keep up with your monthly Compliance tasks.
If you are not using the SmartRIA portal, please let us know so we can find you a more effective solution! Contact Sara Sparks at 303-797-0550, Ext. 3.

CCO CHECKLIST ATTACHED

Finding it hard to login and document your monthly tasks and review oversight on SmartRIA? We have a solution! Refer to the attached checklist- Just print it out, and work through the task reminders. Be sure to retain this checklist in your "Testing" Compliance Files.

AUGUST FOCUS: **Review of Terminated Investment Adviser Representatives**

When someone leaves the company, supervisors are quick to grab the company issued laptop and/or phone. But what about the data on other equipment? How can the organization know what is on his/her mobile devices? Are firms aware of what websites and cloud-based software the IAR has access?

CRP has developed a *SAMPLE Terminated SP Checklist* to assist with the review of Terminated IARs. This will help CCO's with documenting the review of what steps were taken when an IAR of the firm departs.

Examples of some of the access levels to consider when terminating an IAR:

- *Internal IT network*
- *Firm phone, laptop, building access cards*
- *External website access - banking systems, website analytics, blogs, stock photo sites, social media sites*
- *Client account access, trading access*
- *Access to the custodian, third party billing system*

CCO TIP:

- **Tailor and develop a Terminated SP Checklist to ensure a process is in place for review of Terminated Persons (*Refer to our attached SAMPLE checklist*)**
- **Create, maintain on file, and regularly update a central database system that records all the access rights granted to an IAR/employee**

THIS MONTH IN COMPLIANCE
Review of Terminated IARs, SEC Commentary on FORM CRS Filings
Review of Third-Party Vendors

SEC Statement by the Staff Standards of Conduct Implementation Committee Regarding New Form CRS Disclosures

The SEC staff released a Statement on Monday, July 27th regarding the agency's review of a cross section of firms filing the new required Form CRS, or client relationship summary. The SEC Standards of Conduct Implementation Committee said that firms were generally meeting the Form CRS requirement, but they were also noticing problems. Due to the noted problems, the committee plans to host a roundtable in the fall where it will provide more guidance on how firms can improve their Form CRS disclosures. In the meantime, it pointed to online sources of help, such as the instructions for drafting the form and frequently asked questions. CRP will be monitoring the comments and exam findings of firms and communicate any updates to our clients. Continue to stay tuned to our monthly publication for any additional information if we find it necessary to communicate to our clients.

To read the complete SEC Release – https://www.sec.gov/news/public-statement/staff-form-crs-2020-07-27

Importance of Third-Party Vendor Due Diligence

In observing some of the focus areas of recent SEC exams this year, CRP wants firms to ensure there is a process of initial and ongoing review of third-party vendors engaged by the firm. More specifically, CRP highlights a large push for reviewing what these third-party vendors have in place if their operations were disrupted. Outsourcing by financial services companies has unique risks compared to those faced by companies in other sectors. Any errors by third-party vendors in the financial services industry can lead to far greater financial losses than errors in other industries.

Let us address some areas of focus:

- Conduct due diligence when selecting a service provider – ***Sample Review Checklist attached***
- Actively supervise and monitor each essential service provider – ***Maintain a list of all vendors engaged by the firm***
- Ensure that there is a business continuity plan for each vendor. – ***Obtain a copy for your firm's files and document review***
- **Determine if the third-party vendor is essential to business operations. If so, determine if a deeper review of the vendors continuity plan is required.** Review items including a description of the physical security, disaster recovery, back up/redundancy, and prevention features of the company's data center - ***Obtain a copy for your firm's files and document review***
- Assess the legal and regulatory requirements arising from each outsourcing arrangement – ***Review the Service Agreement in place and identify any conflicts or issues with each arrangement, if any***
- Protect confidential information – ***How are these firm's protecting your client's data if shared to facilitate the everyday servicing needs of your clients? Review the Privacy section and Cyber protocols within each Vendor's Agreement to identify any potential issues or lack of protection of client data***

With the SEC's increased attention to third party relationships and your firm's ongoing efforts in reviewing the Risk Matrix this quarter, we recommend spending time on the review of outsourcing arrangements and documenting the review of the vendors with client personal information engaged by your firm. This also applies to those outsourcing arrangements entered by a firm's branches or its associated persons. If your firm decides to use third-party support, *including advisers or sub-advisers*, it is vital that the firm conducts extensive due diligence and oversight. The implementation of adequate controls should ensure that the information used by the firm and distributed to investors is accurate and not misleading. Relying on third parties can put you and your firm at risk for enforcement actions.