Compliance Tips for COVID 19- RIA Compliance Consultants webinar 3/26/2020

- Notify clients of office closing
- Explain how they can contact the applicable supervised persons
- Consider options on how to monitor mail/deliveries if no one is at the office
    - Mail forwarding
    - Daily or weekly pick up by one person
- Remind clients to send securities/checks directly to the qualified custodian (what are their procedures under the current circumstances)
- Notify vendors, if applicable

NASAA established a webpage of COVID-19 updates by state
www.nasaa.org/industry-resources/covid-19-updates/

Single-rep IA firms should review, establish or update temporary service agreement with LPOA and buy-sell agreements with other IA firms, as well as determine what to do if they get sick.

IA should consider, analyze or investigate the implications of COVID-19 on critical operational relationships with key service providers.

Client communications

- Check in with all clients
- Document all communications/meetings (suggest 2nd staff member on call to take notes)
- Utilize agendas/checklists, notes & follow-up emails, letters or minutes
- Trusted emergency contact authorization – don't rely upon custodian
- Verify with client that beneficiaries are correct
- Make sure power of attorneys, health directive, trusts and will up-to-date
- Warn clients of COVID-19 scams related to miracle drugs/remedies
- Warn clients of stimulus package related scams – sharing SSN or account number
- Remind supervised persons to watch for diminished capacity and financial exploitation and to report any to CCO for investigation
- Remind supervised persons to verify 3rd party transfer requests

Text messaging, social media messaging and/or Slack communication with clients

- Does your IA have technology to supervise & archive?
    - If yes, need compliance manual section & training
    - If no, remind supervised persons cannot use text message for client communication or trading purposes

Emails sent to multiple clients should be reviewed as advertising/sales literature

Working Remotely

Physical Security

- Implement clean desk policy – no confidential client information or documents on unattended desk
- Implement procedures to shred immediately any discarded document with confidential client information

Cybersecurity

- Require employees to use firm's computer/laptop
- Encrypt computer/laptop
- Make sure firewall turned-on & anti-virus malware active
- Lock screens when not in use
- Do not write passwords down next to computer
- Have IT use remote access to verify set-up correctly if new arrangement
- Verify not using public wifi
- Use hot spot from phone if necessary
- Verify wifi is password protected (not using factory-installed password), only used by trusted family members and other security features are turned on
- For remote access to server require VPN to access
- Access cloud service providers
    - Turn on 2FA
    - Use unique/complex password

If an advisor is using a personal computer

- Verify operating system and security patches are current and automatically updated
- Make sure firewall is turned on
- Verity anti-virus/malware installed/active
- Create a separate login (if someone else has access)
- Do not save passwords in browser & automatically delete browsing history
- Do not save documents with confidential info on personal computer
- Lock screen or log out when not using
- Recommend requiring employees to confirm in writing and have IT staff check via remote access

Phishing

- Check links before clicking
- Ask others about unexpected emails
- Double check website addresses
- Avoid ads with diagnostic warnings, prize notices or sensational headlines
- Investigate suspicious websites
- Verify site's security
- Secure browser
- Install anti-phishing toolbar in internet browser
- Check online accounts and statements
- Change passwords
- Keep browser updated
- Use firewalls
- Block email pop-ups
- Utilize anti-virus software
- Monitor security breaches involving email access

If there is a breach:

- Contact CCO
- Maintain copy of cybersecurity incident response plan at home

If firm's financial conditions decline:

- SEC – must disclose to clients
- State – must make sure they are still meeting state financial requirements

Client complaints

- All should be reported to CCO
- Review emails/messages/correspondence for complaints
- Promptly ack receipt off any client complaint in writing, conduct investigation, consult with legal counsel, report to E&O, provide letter of findings to client

Email on a breach list:
Subscribe to firefox monitor – allow you to monitor whether your email addresses have been involved in a cyber breach exposing your personal information