Trustmont Group

Plotting the Course:

January 2019

INDUSTRY NEWS: ADVISOR TEXTING AND SOCIAL MEDIA APPS

The Securities and Exchange Commission's Office of Compliance Inspections and Examinations released a risk alert last month concerning the use of mobile devices by investment advisors to communicate with clients through social media, texting and other types of electronic messages. The SEC later announced it named a new deputy director, Daniel Kahl, for the office overseeing this area of focus. The SEC performed a survey to gauge whether advisors were following required policies when engaging with clients, such as keeping copies of communications between client and advisor related to security executions and performance, according to the alert. An increase in the amount of electronic messaging taking place is of concern, according to the SEC, which said in the alert that there has been an increase in volume, citing articles on electronic messaging trends and compliance challenges.

Some examples of SEC recommendations

- Forbid the use of apps that allow advisors to send messages anonymously.
- Advisors should be trained on policies and procedures regarding electronic messaging. Also, make each of them sign a document saying they will comply with the internal rules.
- Hire a software vendor to monitor and archive the use of social media and personal email and messaging by the firm's staff.
- Require that employees gain approval before they can access the firm's email server using their personal devices.
- Load cyber security apps and software on personal and firm-issued mobile devices before they can be used for business communications

***Source: National Exam Program Risk Alert**

Trustmont policies prohibit the use of texting by its registered representatives and advisors unless those messages are being reviewed by Compliance and archived by our service provider, Erado. If you have an interest in being placed into the Erado system, please notify the compliance department.

COMPLIANCE AND OPERATIONS FOCUS

Cyber Security: Email

New email viruses are released almost daily – any one of which can spread throughout your system within minutes. Cyber threats are constantly evolving and are becoming more sophisticated. Over 77% of malware installations come from email, and according to BAE Systems, just 10 malicious targeted emails guarantees a breach because of the effort cyber thieves take to make messages look so real - like they have come from a reliable source.

Not surprising that we have noticed an uptick in the number of emails being reported that contain suspicious content.

Safety tips to remember when utilizing email

- ✓ Change your password often.
- ✓ Use strong passwords. Never use a password that contains "password" or "letmein".
- ✓ Use a different password for each of your accounts. If you use the same password for your bank account as you do for your email account, you become much more vulnerable to data theft.
- ✓ Don't open an attachment unless you know who it is from and are expecting it.
- ✓ Be cautious about email messages that instruct you to enable macros before downloading Word or Excel attachments.
- ✓ Use anti-virus software on your local machine, and make sure it's kept up-to-date with the latest virus definitions.
- ✓ If you receive an attachment from someone you don't know, don't open it. Delete it immediately.
- ✓ Learn how to recognize phishing
  - Messages that contain threats to shut your account down
  - Words like "Urgent" – false sense of urgency
  - Requests for personal information such as passwords or Social Security numbers
  - Forged email addresses
  - Poor writing or bad grammar
- ✓ Hover your mouse over links before you click on them to see if the URL looks legitimate.
- ✓ Instead of clicking on links, open a new browser and manually type in the address.
- ✓ Don't give your email address to sites you don't trust.
- ✓ Don't post your email address to public websites or forums. Spammers often scan these sites for email addresses.

Spam can be more than just an annoyance. It often carries malicious software. And, in the guise of a legitimate message, spam can direct unknowing recipients to websites that silently deposit malicious files or viruses.

- ❖ Don't click the "Unsubscribe" link in a spam email. It would only let the spammer know your address is legitimate, which could lead to you receiving more spam.
- ❖ Don't reply to spam. Be aware that if you reply to a spam email, your reply most-likely will not go back to the original spammer because the FROM header in the spam message will most-likely be forged.

If you suspect that you have been the victim of a security breach, please notify the home office immediately.

IDENTIFYING THE WARNING SIGNS OF FINANCIAL EXPLOITATION

Financial exploitation occurs when a person misuses or takes the assets of a vulnerable adult for his/her own personal benefit. This frequently occurs without the explicit knowledge or consent of a senior or disabled adult, depriving him/her of vital financial resources for his/her personal needs.

Following are some warning signs for you to be aware of:

Client Behavior

- Confused about "missing" funds
- Unable to remember transactions or signing documents
- Exhibits lack of concern regarding risks, commissions, or other transaction costs
- Lying about the reason for the transaction, or who the transaction is to
- Isolation from friends and family
- Abruptly changing their will or beneficiaries

Account Activity

- Account activity that is unexplained, not typical, and/or inconsistent with client's objectives
- Large withdrawals
- Transfers to suspicious parties or foreign countries

- Transfers to a third party that start small, then increase over time
- Transactions that appear to be structured to avoid the $10,000 government reporting requirements

Other Warning Signs

- Signs of client intimidation or reluctance to speak, especially in the presence of a caregiver
- Signs of neglect and/or abuse
- Inability to contact the vulnerable client
- Unpaid bills, despite adequate income
- Family members who were previously uninvolved with client suddenly appear claiming rights
- Someone cashing checks without authorization
- Someone forging signatures
- Unexplained change of address
- Improper actions by fiduciaries (conservators, guardians, trustees, attorneys-in-fact, etc.) *i.e. a power of attorney trying to change themselves to the sole beneficiary*
- The client appears to be victim to a scam *i.e. the client wants to transfer money to an account in order to obtain their "lottery" winnings*

***Source: Senior Financial Exploitation Manual**

If you suspect or are concerned that a customer may be in danger of financial exploitation, please call the home office immediately.

SIX MISTAKES ADVISORS MAKE WHEN ONBOARDING NEW CLIENTS

1. Not sticking to your processes
2. Failing to document client goals
3. Not listening to your team's concerns about particular clients
4. Ignoring investment philosophy differences
5. Not speaking in terms clients understand
6. Accepting clients you know will be trouble

COMPLIANCE REMINDERS

Professional Designations must be approved prior to use on business stationary, business cards, advertising, social media, etc. Approved designations are granted only from organizations that require formal certification procedures including examinations and continuing professional education credits.

Five Star Wealth Advisor is not approved for use by registered representatives and advisors for the above reason.

Some items that must be approved prior to use

- ✓ Social Media Accounts
- ✓ Financial Planning Software Systems
- ✓ Client Record Management System
- ✓ E-fax Systems
- ✓ Call Compliance prior to entering into any contracts.

NEWS AND ANNOUNCEMENTS

The updated **Website** is now published! Check it out at

trustmontgroup.com

Next Mandatory Webinar

Thursday, February 14 at 2 PM EST

New Registered Representative

Thomas Nixon

Upcoming Birthday wishes to

Lacey Dochinez (February 11)

Missy Cosharek (February 23)

Jessica Hartman (April 4)