Monitoring Use of Personal Devices to Work – Best Practices for Broker Dealers

By Victor Peña, Thomas DeMayo and Eric Gelb

In 2020, more than two-thirds of company employees used personal communication devices for work, according to recent estimates. The greater the number of people working remotely due to the pandemic, the greater the risk that the use of personal devices may trigger noncompliance with FINRA and SEC rules on communications oversight. Therefore, it's essential that organizations offer regular training and device monitoring to help meet regulatory requirements while adapting to today's new work environment.

This is especially true in the financial services industry, and in particular the brokerage and Registered Investment Advisor sectors. As the pandemic continues to blur the lines between business and home life, working remotely complicates a firm's ability to monitor and maintain compliance with regulatory requirements regarding client communications. Although this has always been a concern, clearly the new work landscape has brought this issue to the forefront.

There are a variety of reasons that registered representatives may use personal devices to conduct business. In some cases, communicating by text has become so common and convenient that a conversation may evolve from personal to business, and a representative may not even realize that they are using a channel that is not covered by the firm's policies and procedures. Nevertheless, doing so violates firm rules and FINRA regulations. To protect their firms and employees, it's critical for broker-dealers' management to analyze company business practices. Specific problems to identify and address include:

Inability to Monitor Client Communications – The risk is significant when registered representatives and other associated persons use their personal devices to conduct client business. At many companies, these devices are not firm-approved. If they are approved, the firm's communication policies and procedures may not cover the necessary channels of communication such as social media, texting and chatting applications. In addition, capturing and monitoring each representative's remote mediums of client communication present additional compliance risks and challenges that are less likely to be present in structured in-office communications settings.

Supervisory Problems – Although pre-pandemic policies and procedures may have been appropriate to assure adherence to customer communication monitoring requirements, a remote workforce triggers the need to ensure existing policies and procedures address the added risks. In today's new environment, it is imperative that firms review and discuss the recordkeeping and retention details included in FINRA Rule 3110 on Supervision and FINRA Rule 4511.

Best Practices

- Review your Policies and Procedures Manual to ensure it outlines clear guidelines and requirements regarding the use of personal devices to conduct business. Create, implement and continuously review new policies as the remote working environment continues to evolve. This is underscored in the SEC's Division of Examinations' *Risk Alert, Select COVID-19 Compliance Risks and Considerations for Broker-Dealers and Investment Advisors* issued in August 2020. More specifically, it states that "*firms may wish to modify their practices to address the various areas impacted by telework, including communications or transactions occurring outside the firms' systems due to personnel working from remote locations and using personal devices.*"

- Evaluate whether your supervisory and monitoring efforts already include social media and messaging apps (such as Facebook, Instagram and WhatsApp) and if they do, ensure that they cover the ones your representatives may be using. In its *Regulatory Notice 17-18*, FINRA has explained that *"every firm that intends to communicate, or permit its associated persons to communicate, with regard to its business through a text messaging app or chat service must first ensure that it can retain records of those communications as required by SEA Rules 17a-3 and 17a-4 and FINRA Rule 4511."*

- Instruct your firm's IT Group to implement supervisory systems that identify the use of personal devices. If the firm does not have an IT group, consider engaging a qualified third- party to assess the current system and assist in implementing required modifications.

- Review your firm's e-mail monitoring service and settings (both volume and frequency) to ensure that the firm is capturing business activity and unmonitored activity.

- Implement key word surveillance protocols to identify potential troublesome communications and if possible, implement a text messaging monitoring services such as Global Relay and Smarsh.

- Hold regular training sessions – online, via videoconference calls and, once practical, in-person – to inform and update your staff about rules and regulations as well as best practices relating to the use of personal devices. Be sure to cover what is acceptable behavior – specifically, what a representative can discuss on a personal device and what topics and matters are prohibited. *FINRA's Regulatory Notice 11-39* explicitly states that "*a firm's policies and procedures must include training and education of its associated persons regarding the differences between business and non-business communications and the measures required to ensure that any business communication made by associated persons is retained, retrievable and supervised.*"

- Continue to review the adequacy of existing mock exams and branch inspections, most of which are currently being performed remotely using videoconferencing and other technological tools.

Contact Us

These are the steps vital to assuring compliance in today's unexpected and unprecedented remote working environment. As always, our specialists are prepared to help you monitor and identify potential concerns and move quickly to resolve them.

For more information about compliance, personal device management, monitoring and cybersecurity, contact a member of your client service team or:

Victor Peña, CPA, CGMA
Partner
vpena@pkfod.com

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Principal
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com

Eric Gelb, CPA
Senior Managing Director
egelb@pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, fourteen offices in New York, New Jersey, Florida, Connecticut, Maryland and Rhode Island, and more than 900 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 27th on *Accounting Today*'s 2020 "Top 100 Firms" list. It is also ranked among the top 20 best accounting employers to work for in North America by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.