FINRA Guidance for Mobile Deployments (United States)

**Introduction**

FINRA is the largest independent securities regulator in the United States. It has issued guidance over the last several years that is pertinent to mobile devices deployed at its member firms. This guidance applies to devices that are owned by the firm or by its employees. The following information is intended to help a firm develop FINRA-related policies. However, each firm still needs to conduct its own analysis to establish and maintain an appropriate supervisory system for its electronic communications.

**Regulatory Notice 07-59 (December 2007)**

This regulatory notice provides core guidance around the supervision of electronic communications. For mobile, e-mail is the main source of communications to and from the mobile device. All business e-mail should continue to flow through the corporate e-mail system to preserve established supervision and flagging.

However, a mobile device has additional electronic communication methods, such as personal e-mail, text messaging, and social media apps. These communications can go through networks that cannot be supervised by the firm. It is essential to conduct appropriate ongoing training with specific consequences for non-compliance to ensure that employees are fully educated on the firm’s policies and procedures. On an ongoing operational basis, designated reviewers themselves will require new training in mobile technology to understand the capabilities and restrictions of mobile platforms. Otherwise, they will not be able to adequately perform reviews. A structured approval process and mobile user agreement will also be necessary, since FINRA recommends pre-approval for the business use of personal devices.

The firm can use MobileIron for the following e-mail and approval compliance controls:

- Restrict the ability to forward business e-mail through a personal e-mail account
- Ensure the data on the device is encrypted
- Block unapproved personal devices connecting to the corporate e-mail infrastructure

**Regulatory Notice 10-06 (January 2010)**

This regulatory notice establishes guidance on the use of social media web sites. This guidance does not differ if the endpoint used for social media communications is a mobile device instead of a desktop, or if the endpoint is employee-owned instead of firm-owned. The firm’s policies should clearly state that restrictions on establishing social media accounts for business purposes are the same for a mobile social media app as for a traditional web-based social media site. The firm may need to expand its standard screening process for sites having public posts to include new mobile-driven sites and apps.
Mobile Security and Compliance Strategies

The firm can use MobileIron for the following mobile social media compliance controls:

- Monitor social media app inventory across the firm to understand type and prevalence
- Use MobileIron App Control rules to create disallowed lists of certain mobile social media apps
- Use MobileIron Event Center to notify users of their FINRA obligations upon download of those apps
- Apply tighter rules to devices of users who have presented compliance risks in the past

**Regulatory Notice 11-39 (August 2011)**

This regulatory notice expands guidance on the use of social media and personal devices. This notice makes very clear that devices owned by the employee can, in fact, still be used for business communications as long as those communications are retrievable and separate from personal communications. If this is possible, then the firm is not obligated to supervise all personal communications, as well.

Note that only the content of the communication is relevant in assessing recordkeeping requirements. Whether the device triggering that communication is personal or firm-issued is not relevant. Therefore, as in the above two sections, ongoing training is critical to ensure employees realize that the extensive social media habits they might have formed on their personal device do not apply to business communications.

The firm can use MobileIron for the following personal device compliance controls:

- Control the corporate e-mail profile, restricting forwarding of e-mail through personal accounts, as described in the first section of this document
- If the firm has other communications systems accessible by the employee through the web, then configure VPN through MobileIron to provide secure access for those websites
- If the firm has other communications systems accessible by the employee through mobile apps, then distribute those apps through the MobileIron enterprise app storefront so that they can be tracked and removed if necessary

**Conclusion**

FINRA has expanded guidance in the last few years to specifically address personal devices and social media communications, both of which are very common trends in mobile. The MobileIron platform has several controls that can be part of a FINRA supervisory system to address these areas.

MobileIron allows a firm to manage the enterprise workspace on the mobile device, which includes enterprise e-mail, apps, and connectivity, separately from the user’s personal workspace on the device. MobileIron’s policy enforcement prevents inappropriate communications and provides a closed-loop notification path to educate users of their FINRA obligations. Further papers on MobileIron’s approach to security and compliance for iOS, Android, and Bring-Your-Own-Device (BYOD) programs can be found [here](#).