Guidepost

COMPLIANCE EXPERTS DISCUSS OFF-CHANNEL COMMUNICATIONS AND MOBILE SURVEILLANCE POLICIES

Roundtable Discussion: Off-Channel Communications and Mobile Surveillance Policies

Surveillance, monitoring, escalation, and reporting are critical components to regulatory compliance and risk management. So is consequence management. These are especially important given the major penalties and remedial steps required of banks and swap dealers, and in view of recent US Department of Justice (DOJ) expectations over "Off-Channel Communications".

These regulatory and ethical expectations aren't easy to execute, especially when employees have access to so many modes of video, audio, and social media communications. In our recent roundtable, senior compliance executives from various major financial institutions came together to discuss the challenges they face meeting regulatory and ethical demands for off-channel communications and record retention.

The goal of our discussion was simple: to provide "safety in numbers" where compliance professionals could talk through solutions and help each other out, without attribution and under "Chatham House Rules".

Attendees discussed the scope of their surveillance policies, and who's accountable for enforcing these policies. They debated whether business-issued devices alone, are an effective way to eliminate off-channel communications with clients, and shared other ways their firms are discouraging or prohibiting employees from having unsanctioned contact with clients. They also discussed who is subject to monitoring, how they evaluate breaches of compliance policy, and who takes disciplinary action when there's been misconduct.

Below is a summary of responses to three key questions addressed in the discussion.

Off-channel communications policies: who should own them, and is one, global policy sufficient?

A few of our participants said selecting an effective owner for off-channel communications policies has been a pain point, with ownership extending not only to the policy but also to the controls associated with it. Ownership of these policies has shifted from compliance to cybersecurity, and back again. Ultimately, most participants agree that it makes sense for these policies to at least start with the second line compliance function, as policy owner, with the first line businesses executing the controls. Any risks should then be escalated to business supervisors and compliance for assessment and appropriate action.

When asked about the geographical scope of these policies, most financial institutions in our discussion said they have implemented a global policy with some regional nuances. These policies provide visibility into what is permissible and authorized locally in off-channel communications, but emphasize the importance of recording business interactions, regardless of the region – particularly if businesses cut across geographies.

Ultimately, however, the fundamental principles, such as recording and retaining business communications, remain consistent across regions. While we may see convergence towards a global standard, additional regulation isn't really necessary. Regulators are telling us the same things we've known for years – if you're told you need to record on a medium and you don't, you're going to be subject to some serious sanctions and scrutinized to remediate and upgrade compliance. Any convergence is anticipated to manifest in the penalties imposed internally on individuals who violate policies, not on the policies themselves.

Are business-issued devices effective in preventing off-channel communications?

Participants were divided on whether to implement business-issued devices only for employees to conduct mobile client communications. Some financial institutions have ultimately decided not to, because they don't think a business-issued phone will prevent anyone from using their personal phone if that's what they want to do. Others think business phones do at least act as a deterrent, and have either already adopted business-issued devices, or intend to in the near future.

Those institutions who still allow employees to use personal devices mandate that all business communications occur through a company app, which captures text, SMS, and social media communications. Those that use business-issued phones do not allow employees to download apps beyond what the compliance team has authorized, so that there's no risk of communications on unsanctioned platforms.

In any case, participants agreed that technology alone isn't sufficient to prevent off-channel communications. Firms need to conduct regular training and enforce a stringent definition of what constitutes business communication. At one bank, any and all off-platform communications, however informal, are discouraged and potentially monitored due to the possibility for these conversations to shift to business matters.

Many institutions also have employees submit quarterly attestations, confirming their adherence with off-channel policies, or any violations that may have occurred.

How is compliance with these policies enforced, and is anyone exempt from the rules?

Multiple participants said that policy breaches are assessed by committees. During "conduct" committee or compliance committee meetings, members discuss employees that are continually delinquent in their training, or have violated policies and procedures, and decide whether there are real, more systemic conduct issues. In some cases, when misconduct is identified, the case is escalated to another committee, which deals with consequences.

Interestingly, some firms said that no one, including the CEO, is exempt from monitoring. Others said that their senior leaders are exempt since executive leadership is outside the scope of our regulated entities. And although board members are exempt, one firm said they just rolled out a personal trading policy to this group, too.

A big thank you to everyone who participated in our first roundtable in this series. Hearing so many diverse perspectives on these topics was invaluable, and we look forward to the next session!

ERIC YOUNG

Senior Managing Director

Eric T. Young advises highly regulated organizations on reengineering compliance, ethics, and regulatory technology programs to enable reputable and sustainable business growth. He has deep regulatory experience having spent close to 40 years in chief compliance officer roles at some of the world's largest institutions, including five global banks. Throughout his career, Mr. Young has remediated and transformed corporate compliance programs and financial crime compliance programs including sanctions; integrated compliance and ethics cultures between regions, countries and companies to ensure consistency across enterprises; built compliance budgets; enhanced reporting; created governance frameworks and risk assessment, monitoring and testing programs; closed compliance gaps; restructured compliance teams; and mentored junior staff to create a pipeline of future compliance leaders and enable grassroots compliance ideas, solutions and digital upgrades.