CHECKLIST

How to Inspect Communications for Outside Business Activities

OVERVIEW

Monitoring employee conduct has become more complicated now that work from home seems here to stay. Offices went virtual, business is conducted at home, and now, social media platforms have transformed into the trading-room floor. For wealth management firms under the watchful eye of regulators, employee involvement in unauthorized outside business activities (OBA) like the GameStop debacle could have serious consequences. In fact, in FINRA's 2021 Examination and Risk Monitoring priorities letter, OBA was elevated as a critical issue to which firms should be paying careful attention.

It has never been more important to take proactive steps to increase visibility into employee communications and identify potential misconduct. But it requires a thorough review of existing policies and procedures and making changes to fit the current (and future) communications landscape. This checklist will help you identify potential areas of OBA risk and close the visibility gap for unauthorized business activities and other areas of employee impropriety.

Obligations for monitoring broker-dealer OBAs

FINRA RULE 3270
(Outside Business Activities of Registered Persons) requires registered representatives to notify their firms in writing of proposed outside business activities (OBAs), so firms can determine whether to limit or allow those activities.

FINRA has noted several key considerations for monitoring the OBAs of registered representatives. To update your firm's policies and procedures regarding OBAs, begin by asking the following questions:

- [ ] Do your firm's Written Supervisory Procedures (WSPs) explicitly state where notification or pre-approval is required to engage in an OBA?
- [ ] Does your firm require associated persons or registered persons to complete and update, as needed, questionnaires and attestations regarding their involvement—or potential involvement—in OBAs, and if yes, how often?
- [ ] Do you have a process in place to update a registered representative's Form U4 with OBAs that meet the disclosure requirements of that form?
- [ ] What methods does your firm use to identify individuals involved in undisclosed OBAs?
- [ ] Does your firm take into account the unique regulatory considerations and characteristics of digital assets when reviewing digital asset OBAs?

How to proactively manage employee misconduct with policies

Outside business activities are a required area of accountability for financially regulated firms and registered representatives. However, many other organizations can benefit from taking a proactive posture toward improving visibility into the outside business activities of their remote employees, especially on company time, devices or networks. Lacking explicit guidance, distributed work teams can engage in misconduct—via easy access to an infinite number of collaborative, messaging and mobile application platforms—that can cause major issues for any business.

Following the practices on this checklist will help you identify policy infractions and protect your organization.

☐ Tune acceptable use policies

Execute policy tuning to explicitly address which communication tools are acceptable for business use, including the use of data on public forums. Outline consequences for prohibited use.

☐ Inspect record retention policies

For many firms, the definition of what constitutes a "business record" was established when records were paper-based or exchanged via email or enterprise content management systems. Given today's dependence on digital collaborative and messaging technologies, now is a good time to reopen the debate between compliance, legal and IT as to what constitutes a record in a world of voice, video, whiteboards, and persistent chats on mobile devices. While there are no easy answers or a "one size fits all" policy set, waiting for explicit regulatory guidance to determine retention strategies is now a much riskier proposition. Ensuring that retention policies reflect where business is happening today will also dramatically reduce the effort in inspecting content for possible outside activities later.

☐ Upscale third-party risk assessment programs

Today's content lives in the cloud and runs on platforms whose vendors have varying levels of understanding of your regulatory and information governance objectives. Dependence on a technology vendor with inadequate security, privacy and other data protection controls raises the risk that a complete record of historical communications activities can be sustained and investigated when required.

☐ Create location-blind Codes of Conduct

Ensure Codes of Conduct are sufficiently expansive to address (or not unintentionally exclude) situations that can arise around a water cooler, in a conference room, or in an online meeting to ensure applicability in working from an office, home, on the road, and mixed environments.

☐ Update training programs

Training should reflect the specific set of features that each approved communications and collaborative tool provides, as well as the role of the individual as a regulated vs. non-regulated, client facing vs. back-office employee, etc. Clearly delineating where the boundary exists between business and personal use of platforms that can be used for both should also be central to updated programs.

☐ Update supervisory OBA policies

For regulated users, firms should ensure current supervisory policies address the many ways their representatives may engage in outside business activity. Many firms limit communication channels their employees are allowed to use. This is because every new channel creates: increased review burden, a need for targeted lexicons reflecting the unique jargon and communication styles of different platforms, and the complexity of following ongoing conversations across devices. But limiting the channels through which your firm interacts with retail investors also limits your level of insight into the various demographics represented in the market. Well-crafted policies and lexicons targeting a variety of outside business activities, and that reflect multi-channel communication, help bridge the gap while giving firms valuable tools to mitigate risk.

☐ Monitor prohibited networks and devices

Often highlighted in regulatory enforcement actions, the use of unapproved personal devices and networks have frequently found their way into the news. These mishaps have included unauthorized outside business activities, fraud, promising investment returns and sharing non-public information. With a robust supervision solution, automated policies can flag messages containing certain words or phrases likely to warrant review or indicate the use of prohibited networks. In addition, we recommend monitoring social media, professional networking sites and other sources such as legal research databases and court records for misconduct.

EXAMPLES OF POLICY PHRASES TO MONITOR:

- “Send to my Gmail”
- “Respond to my personal email”
- “Text me”
- “Let’s take this offline”
- “PPP loan”
- “Side gig”
- “Volunteer position”

☐ Expand supervisory spheres

Firms that have regulatory obligations to retain and supervise employee communications may have thought of (or still consider) those obligations as a resource drain and tax on the business. Ironically, these same firms are now in an advantageous position to apply supervisory disciplines and infrastructure beyond regulated user pools. They can expand their supervisory spheres to others in the firm that have access to high-value or sensitive information, those with a history of misconduct, or the people with whom either of those groups frequently communicate.

☐ Leverage advances in content surveillance technology

Investigating communications for potential outside business activities has at least two potential challenges: 1) those intent on wrongdoing will tend to go where they believe they can avoid detection, and 2) each of these content sources is unique, with their own syntax, available method of capture and inspection, and features to mask activity such as encryption. Finding content needles in multiple data haystacks can stretch human, lexicon-based content review past their useful limits. Leverage of existing supervisory tools and processes can be used to spot red flags, which then can be further analyzed for patterns and behaviors by surveillance technologies.

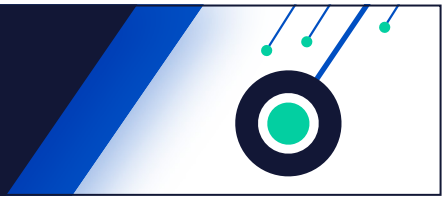
Anticipate the next network

We've all witnessed an acceleration in collaboration and messaging technologies in response to the work-from-home reality. That won't change any time soon. Firms need to respond with regular testing and audit of systems and processes, and their applicability to new communications sources introduced in the market.

As illustrated by the GameStop case, reduced visibility into employee behavior combined with the plethora of increasingly diverse communication platforms, provides a pathway to the next generation of employees' outside activities or other misconduct. And those misdeeds will likely be conducted over tools or applications we've not yet heard of. Now is the opportunity to adopt a proactive posture before missing an activity that could damage the firm and produce negative regulatory and legal outcomes.

LEARN MORE

Definitive Guide to Electronic Communications Supervision



smarsh®

Smarsh® is the recognized global leader in electronic communications archiving solutions for regulated organizations. The Smarsh Connected Suite provides innovative capture, archiving, e-discovery, and supervision solutions across the industry's widest breadth of communication channels.

Scalable for organizations of all sizes, the Smarsh platform provides customers with compliance built on confidence. It enables them to strategically future-proof as new communication channels are adopted, and to realize more insight and value from the data in their archive. Customers strengthen their compliance and e-discovery initiatives, and benefit from the productive use of email, social media, mobile/text messaging, instant messaging and collaboration, web, and voice channels.

Smarsh serves a global client base that spans the top banks in North America and Europe, along with leading brokerage firms, insurers, and registered investment advisors. Smarsh also enables federal and state government agencies to meet their public records and e-discovery requirements. For more information, visit www.smarsh.com.

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions. You must consult your attorney regarding your compliance with applicable laws and regulations.

US: 1-866-762-7741 | UK: +44 (0) 20 3608 1209 www.smarsh.com @SmarshInc SmarshInc Company/Smarsh