ALSTON & BIRD

WWW.ALSTON.COM

White Collar, Government & Internal Investigations / Privacy, Cyber & Data Strategy ADVISORY ■

OCTOBER 12, 2023

The Latest in the SEC's Off-Network Communications Enforcement Sweep

by Kate Hanniford, Paul Monnin, and Albert (BJ) Stieglitz

On September 29, 2023, the U.S. Securities and Exchange Commission (SEC) announced enforcement actions against five broker-dealers, three dually registered broker-dealers and investment advisers, and two affiliated investment advisers for what the SEC described as "widespread and longstanding failures to maintain and preserve electronic communications." The enforcement actions, settled by each respondent, included fines ranging between $2.5 million to $35 million, as well as remedial actions like retention of an independent compliance consultant, mandatory reporting of any disciplinary actions, and review of employee communications as a regular internal audit item.

These settlements are the latest in the SEC's sprawling investigation of its registrants' use of off-network communications, which has included enforcement actions against 30 other firms over the past 24 months, and has been the subject of previous client updates here and here.

Key Takeaways

Continued scrutiny of investment advisers

The SEC's ongoing aggressive enforcement of recordkeeping violations continues to focus on investment advisers, despite their trade associations' contention in correspondence to the SEC that agency jurisdiction to police custody of business-related communications is confined to broker-dealers. Recent investment adviser settlements show that advisory entities have been willing to waive this defense, however, given the prospect of increased penalties following a litigated proceeding.

Content is a focus

While the SEC will continue to penalize registrants that fail to control use of off-network communications, the agency has apparently entered a new phase of its enforcement initiative. Reports indicate that the SEC has directed large advisory entities to share messaging data from senior management and other key employees' devices – collected as part of their internal investigations – in response to the SEC's off-network communications sweep.

Although the disclosed data, specifically WhatsApp and other messaging application information, is reportedly limited to business-related communications, the exchange of material, nonpublic information or other evidence of suspected fraud and abuse is plainly fair game. Similar to the insider trading push that emanated from the capture of trader texts and other out-of-band communications following the market turmoil caused by the Great Recession, the SEC clearly intends to data-mine the WhatsApp and other messaging information it has received to pursue more than just compliance violations. And to the extent it can establish a beachhead in one firm, those who traded with that firm should also expect regulatory attention extending beyond mere recordkeeping scrutiny.

Compliance is ever more important

The SEC continues to target primarily endemic recordkeeping failures – including by gatekeepers and at the senior levels of management. Although one respondent discovered its violation through its internal compliance department and ultimately self-reported (resulting in a substantially lower fine), most of the enforcement actions resulted from the SEC's recordkeeping sweep, which it has described as a "risk-based initiative."

Continued Vigilance

Registered firms should anticipate continued and aggressive SEC scrutiny of their off-network business communication policies and should expect that such interest will be a routine feature of regulatory examinations moving forward. To avoid compliance deficiencies, which if significant enough may ripen into enforcement referrals (especially given the degree to which the SEC's enforcement initiative has been highly publicized and continues to expand), registrants should consider the following steps:

- Review existing policy enforcement mechanisms that enable the firm to assess compliance with its policies and procedures and to provide the basis for sanctions where appropriate.
- Review employee training modules, including the assessment of whether employees understand and have attested to their understanding of firm policy.
- Test the firm's capacity for archiving, surveillance, and overall compliance with stated policies and procedures.
- Review current technical solutions to confirm they are reasonable and appropriate.
- Using a risk-based approach, identify functions or personnel whose messaging communications may present heightened compliance risk to the enterprise and apply enhanced procedures to mitigate the risk.

Moreover, now that the SEC has moved beyond the mere fact of off-network communications to an investigation of their substance – using WhatsApp and other apparently unvarnished messaging data collected from strategic employees' devices to get there – simply closing compliance gaps may no longer be enough. In addition to compliance imperatives, firms need to take a risk-based approach to investigating the substance of trader and client-facing communications that occurred off-network. This includes surveying employees about use of private messaging and imaging devices that have been supplied to employees or employee-owned devices that house business information. This requires care in observing privacy limitations, while also understanding that putatively private applications are where evidence of potential fraud and abuse is mostly likely to be found.

You can subscribe to future ***White Collar, Government & Internal Investigations*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any member of our White Collar, Government & Internal Investigations or Privacy, Cyber & Data Strategy Teams.

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: Vantage South End ■ 1120 South Tryon Street ■ Suite 300 ■ Charlotte, North Carolina, USA 28203-6818 ■ +1 704 444 1000 ■ Fax: +1 704 444 1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: City Center Fort Worth ■ Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ +1 214 922 3400 ■ Fax: +1 214 922 3899
LONDON: LDN:W ■ 6th Floor ■ 3 Noble Street ■ London ■ EC2V 7DE ■ +44 20 8161 4000
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 755 Page Mill Road ■ Building C - Suite 200 ■ Palo Alto, California, USA 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333