



Investment Management, Trading & Markets / White Collar, Government & Internal Investigations ADVISORY ■

MARCH 16, 2022

SEC and CFTC Crackdown on Use of Personal Messaging Platforms Raises Compliance Concerns – and Opportunities

Recent disclosures by several of the world's largest financial institutions indicate that the Securities and Exchange Commission's (SEC) and Commodity Futures Trading Commission's (CFTC) scrutiny of the use of unapproved messaging platforms for business communications continues across the industry. This follows these agencies' recent enforcement actions against a broker-dealer subsidiary of a major U.S. financial institution, accompanied by the "invitation" to other industry participants to self-disclose their own use of personal devices for business purposes, without mention of any potential safe harbor or cooperation credit.

The SEC's and CFTC's willingness to bring enforcement actions based solely on underlying violations of records retention rules signals a more aggressive near-term enforcement posture in this space. Given the prevalence of personal (and ephemeral) messaging platforms and the rigors of statutory and regulatory requirements such as those found in the Exchange Act and the SEC's Compliance Rule, this more aggressive posture further underscores the critical importance for the broker-dealer and investment adviser community of ensuring the adequacy and effectiveness of recordkeeping policies and procedures and otherwise continuing to take measures to strengthen compliance programs.

Records retention practices related to the intersection of business communications and personal messaging applications will soon feature in SEC examinations, more formal enforcement investigations, and even in whistleblower claims. Leveraging the lessons of recent enforcement activity and agency guidance regarding compliance with recordkeeping requirements will enable firms to adjust their compliance programs to mitigate this heightened enforcement risk.

Industrywide Scrutiny and Additional Enforcement Risk

Any hope that the SEC's and CFTC's recent enforcement actions based on use of personal messaging platforms—including personal text messages, WhatsApp messages, and personal emails—to communicate about business matters might be a one-off has proven to be misplaced. A series of recent disclosures by a number of global financial institutions indicates that the SEC and CFTC have contacted these firms about their use of unapproved messaging systems or that these firms have proactively initiated their own reviews. While the ultimate outcome of this enforcement scrutiny is uncertain, its breadth signals the SEC's and CFTC's appetite for additional enforcement actions based on similar violations and also has implications beyond the messaging-related investigations themselves.

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

For example, entities currently subject to the terms of a deferred- or nonprosecution agreement, as well as entities facing Department of Justice (DOJ) scrutiny for matters entirely unrelated to recordkeeping, may be questioned by the DOJ about whether they have implemented “appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company’s ability to appropriately retain business records or communications or otherwise comply with the company’s document retention policies or legal obligations.” Failures of the sort identified by the SEC and CFTC in their current enforcement initiative could heighten enforcement risk from other agencies. And if the use of personal messaging occurs in connection with suspect trading patterns or other suspicious conduct, it may considerably expand that risk.

Opportunities to Identify and Close Compliance Gaps

Financial firms should anticipate that the SEC and CFTC will continue to focus on appropriate recordkeeping in examinations and, as may now become more likely following recent enforcement actions and disclosures by other industry participants, in response to whistleblower complaints. In addition, a firm’s ability to demonstrate acquisition and retention of electronic communications from diverse sources may also arise in the context of regulatory investigations, including in response to subpoenas and in connection with investigative testimony.

This renewed enforcement focus on the surveillance, retention, and retrieval of electronic communications provides opportunities for firms to revisit current practices and to consider whether additional mitigation may be appropriate. Among other things, firms should:

- Review their bring your own device (BYOD) policies and user acknowledgements to ensure that the firm’s ability to monitor, obtain, retain, and review communications is clear and in compliance with applicable U.S. or other foreign laws, as appropriate.
- Review the firm’s acceptable use or similar, user-facing policies that make clear that firm information is firm property (regardless of where it is stored) and therefore needs to be accessible to the firm.
- Review applicable agreements with third-party messaging service providers as well as their surveillance and storage capabilities and configurations to be sure these providers are retaining communications in a format that can be monitored, retrieved, archived, and backed up compatibly with the firm’s other technology resources.
- Review and test the firm’s ability to retrieve the various approved electronic communications from backups.
- Consider whether additional data mapping may be helpful to ensure that the firm has identified all approved electronic communications and that these are accessible for purposes of regulatory compliance.
- Review training modules to ensure employees understand stated policies and procedures for limitations on the use of personal electronic communications and the monitoring, retention, and potential uses of those electronic communications.
- Review employee attestation and disciplinary policies to ensure employees both attest to their compliance and understand the sanctions for noncompliance.
- Consider implementing or enhancing an audit, review, or follow-up mechanism to verify that firm supervisors are ensuring compliance with stated policies and procedures.
- Review the firm’s ability to assess emerging electronic communications platforms that may be attractive to employees and its process for considering and approving or preventing such communication methods.

Use of personal devices and messaging platforms for business purposes is both convenient and ubiquitous. While federal agencies recognize the compliance challenges posed by these practices, as evidenced by their [guidance](#), the SEC's and CFTC's recent activities—including their recently settled enforcement actions and their reportedly ongoing investigations of similar conduct at other institutions—nevertheless demonstrate that firms may be held accountable for the use of unapproved electronic communications by employees in the ordinary course of business.

Although compliance challenges associated with identifying unapproved communications and assessing new technologies will persist, proactive assessment and mitigation of issues related to the surveillance, retention, and retrieval of electronic communications will pay dividends in limiting enforcement risk.

You can subscribe to future *Investment Management, Trading & Markets* and *White Collar, Government & Internal* 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 of the following:

Investment Management, Trading & Markets Team

David J. Baum
202.239.3346
david.baum@alston.com

Katherine Doty Hanniford
202.239.3725
kate.hanniford@alston.com

Saloni Joshi
+44.020.3823.2197
saloni.joshi@alston.com

Dustin J. Littrell
214.922.3475
dustin.littrell@alston.com

Martin H. Dozier
404.881.4932
martin.dozier@alston.com

Kristin P. Hinson
704.444.1332
kris.hinson@alston.com

Joel Jung
212.210.9564
joel.jung@alston.com

Timothy P. Selby
212.210.9494
tim.selby@alston.com

Blake E. Estes
212.210.9415
blake.estes@alston.com

Colby B. Jenkins
704.444.1280
colby.jenkins@alston.com

Megan Lau
+44.0.20.3907.1288
megan.lau@alston.com

Helena Wong
212.210.9464
helena.wong@alston.com

Timothy C. Foley
202.239.3741
timothy.foley@alston.com

White Collar, Government & Internal Investigations Team

Joanna C. Hendon
212.210.1244
joanna.hendon@alston.com

Brian D. Frey
202.239.3067
brian.frey@alston.com

Meredith Jones Kingsley
404.881.4793
meredith.kingsley@alston.com

Jason D. Popp
404.881.4753
jason.popp@alston.com

Edward T. Kang
202.239.3728
edward.kang@alston.com

Michael R. Hoernlein
704.444.1041
michael.hoernlein@alston.com

Jenny Kramer
212.210.9420
jenny.kramer@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

R. Joseph Burby IV
404.881.7670
joey.burby@alston.com

Joseph H. Hunt
202.239.3278
404.881.7811
jody.hunt@alston.com

Emily McGowan
704.444.1027
emily.mcgowan@alston.com

Albert B. Stieglitz, Jr.
202.239.3168
albert.stieglitz@alston.com

Isabelle De Smedt
+32.2.550.3700
isabelle.desmedt@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

Paul N. Monnin
404.881.7394
paul.monnin@alston.com

Thomas G. Walker
704.444.1248
919.862.2212
thomas.walker@alston.com

Byung J. "BJay" Pak
404.881.7816
bjay.pak@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

© ALSTON & BIRD LLP 2022

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 8592 7500
 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: One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
 DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
 FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ 214.922.3400 ■ Fax: 214.922.3899
 LONDON: 5th Floor, Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
 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: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 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