SEC PROBE DEMANDS PERSONAL MOBILE DEVICES

THE PRACTICE MAKES PERFECT

SERIES - 4 / ARTICLE - 5

NOVEMBER 23, 2022

By **Jeffrey Brochin, Esq.**

GreenPoint> Law&Compliance

william.anderson@greenpointglobal.com | pranav.menon@greenpointglobal.com

International Corporate Center, 555 Theodore Fremd Avenue, Suite A102 Rye, NY 10580

www.greenpointlegal.com

You probably thought your WhatsApp and other text messages were safe from the government's prying eyes. If you work in the Wall Street financial sector, that would no longer be true. The U.S. Securities and Exchange Commission (SEC) has launched a wide-reaching probe into the use of 'off-channel' modes of communication by banking industry employees, and yes, personal devices are being targeted. The 'sweep' is ostensibly all part of SEC Commission Gensler's enforcement campaign pertaining to accurate record-keeping. But critics claim the focus on broker-dealer employees' communications on their personal devices raises serious invasion of privacy issues.

Top Executives Targeted

This past May, the SEC began an operation targeting bankers and traders at each major bank it decided to go after, demanding that more than 100 employees and executives turn over their personal mobile devices. The purpose was so that SEC lawyers could examine the devices for WhatsApp chats, text messages, and personal email accounts. The search through Wall Street dealmakers' personal information on over 100 phones is part of a far-reaching probe into the alleged use of 'off-channel' platforms by dealmakers for the exchange of business information.

The sweep of personal mobile devices comes on the heels of a $200 million fine levied against JPMorgan Chase in December 2021, in which a subsidiary broker-dealer of the bank agreed to pay $125 million to the SEC over charges that the bank failed to preserve written communications of its employees and another $75 million to the Commodities Futures Trading Commission (CFTC) in civil money penalties. The bank also consented to a cease-and-desist order regarding further record-keeping violations, and they agreed to various remedial measures.

Investigation Expanded

In the wake of the JPMorgan Chase probe, the SEC decided to expand their examination of private mobile devices and sent 'requests' for messaging app data to Goldman Sachs Group Inc., Morgan Stanley, Credit Suisse AG, HSBC Holdings Plc, and Citigroup Inc., all of whom are reportedly cooperating with regulators. The institutions have hired outside counsel to assist in reviewing the cellphone content in an attempt to filter out private, personal messages from those considered business-related. But how well employee privacy rights can be preserved in the course of this Wall Street messaging hunt is not yet clear.

Pandemic? Or Fear of Spoliation?

When the SEC first launched the campaign last Fall, the explanation offered was that with the rise of telework arrangements due to the Covid-19 pandemic, there were concerns as to whether banks were keeping proper track of digital communications exchanged by work-at-home employees; therefore, it was necessary to ramp up the SEC's enforcement arm to ensure that banks were adhering adequately to documenting employees' work-related communications.

However, the fact is that as far back as 2007, regulations existed allowing fines for records violations related to IM and text messaging. That year FINRA issued Regulatory Notice 07-59, focusing on the context, content, timing, and affected audience of a

> **"AS TECHNOLOGY CHANGES, IT'S EVEN MORE IMPORTANT THAT REGISTRANTS ENSURE THAT THEIR COMMUNICATIONS ARE APPROPRIATELY RECORDED AND ARE NOT CONDUCTED OUTSIDE OF OFFICIAL CHANNELS IN ORDER TO AVOID MARKET OVERSIGHT"**
>
> ***— 'SEC Chair Gary Gensler***

message rather than the platform by which it was transmitted. All of those were factors in determining whether or not a communication was a business communication. In a speech last October, Gurbir S. Grewal, Director of the SEC's Division of Enforcement, cited a more aggressive enforcement of recordkeeping obligations related to preserving off-channel communications on account of such records being "essential to market integrity and enforcement." He also cited the inability of Enforcement to adequately examine financial service companies as causing delay and obstruction of investigations, which raised a broader issue of accountability and spoliation issues.

When the SEC Itself Destroyed Records

There is an ironic, historical footnote to the SEC probe. On June 15, 2011, the SEC's Office of Inspector General (OIG) opened an investigation into allegations the SEC Division of Enforcement had improperly destroyed records relating to Matters Under Inquiry (MUIs) over a twenty-year period and that the SEC made misleading statements in an August 27, 2010 response to a July 29, 2010 letter from the National Archives and Records Administration (NARA) concerning the SEC's potential unauthorized destruction of an MUI records.

The OIG investigation found that for at least 30 years, Enforcement had opened MUIs as "pre-investigation inquiries" and that it was the policy of Enforcement to dispose of all documents relating to a MUI that were closed without becoming investigations. However, the OIG investigation also found that the SEC's Enforcement staff destroyed documents related to closed MUIs that should have been preserved as federal records.

Nothing's Really Private

Given both the existing record-keeping regulations and the SEC Enforcement Division's newest sweep of communications stored on or transmitted over personal cellphones, the fact becomes obvious that business communications in financial services are neither personal nor private. The SEC can—and is—demanding the turnover of employees' personal devices for an inspection at will, and dealmakers throughout the financial sector must be prepared with procedures and technology in place in order to comply with communications record-keeping requirements—regardless of whether internal or external—in readiness for the inevitable regulatory or legal review.

Executive Summary

1. The Issue

The SEC Enforcement Division is demanding that regulated entities turn over employees' private cell phones for 'off-channel communications' inspection.

2. The Gravamen

There is no right of privacy as to the content of one's personal device if it has ever been used for an employer's business communication.

3. The Path Forward

Dealer-brokers must have in place compliance measures related to text messaging or risk multi-million-dollar fines for alleged record-keeping violations.

Action Items:

1 Reality Check:

Start with the basic premise that none of your communications on your personal mobile device are private if you work for a regulated entity in the financial sector.

2 Processes and Technology:

For counsel to the financial sector, clients must be advised as to having in place processes and technology to maintain adequate record-keeping that includes all electronic records.

3 Supervisory Systems:

Financial sector clients must enforce supervisory systems for all business communications, whether internal or external.

4 Regulatory Cooperation:

As discovered by top Wall Street financial giants, when an SEC deep probe does arise, it is highly advisable to extend cooperation to the agency while maintaining the involvement of your own counsel so as to have a monitoring presence as to privacy issues.

Further Readings

1. https://www.morningstar.com/news/marketwatch/20220518463/sec-is-reportedly-checking-banker-cell-phones-in-a-wall-street-messaging-probe
2. https://www.cnbc.com/2021/12/17/jpmorgan-agrees-to-125-million-fine-for-letting-employees-use-whatsapp-to-evade-regulators.html
3. https://www.investmentnews.com/goldman-probed-by-sec-over-messaging-sent-using-unapproved-services-217846
4. https://www.steel-eye.com/news/regulatory-scrutiny-and-fines-ramp-up-for-lax-employee-monitoring
5. https://www.arnoldporter.com/en/perspectives/blogs/enforcement-edge/2021/10/sec-enforcement-turns-focus-to-broker-dealer
6. https://www.smarsh.com/blog/thought-leadership/SEC-reviews-personal-phones-for-business-comms/

Jeffrey Brochin, Esq.

GREENPOINT STAFF COUNSEL
AND CONTENT EDITOR

After receiving his Juris Doctor degree from The John Marshall Law School in Chicago, Mr. Brochin served as an Administrative Law Judge with the Illinois Department of Labor for six years where he presided over cases dealing with job separation issues and matters pertaining to contested Unemployment Insurance claims. He also co-wrote the agency's administrative rules, and periodically served as a 'ghost writer' for Board of Review decisions. Following that position, he was Director of Development for a Chicago-area non-profit college where he was responsible for High Net Worth donations to the institution. For the next eighteen years he practiced as a solo practitioner attorney with an emphasis in the fields of Real Estate law and Commercial Contracts transactions, and was an agent for several national title insurance agencies.

In 2003 he was recruited to head up a U.S. title insurance research office in Israel, a position he held for four years, and between 2007-2017 he participated in litigation support for several high-profile cases. He has taught Business Law as a faculty member of the Jerusalem College of Technology, and has authored a wide variety of legal White Papers and timely legal articles as a professional legal content writer for GPL clients. Separate from his legal writing, he has co-authored academic articles on Middle East security topics that have been published in peer-reviewed publications.

William H. Anderson, Esq.

MANAGING DIRECTOR AND HEAD OF
FINANCIAL PRODUCTS AND SERVICES

William Anderson is Managing Director and Head of Law & Compliance. He leads the GreenPoint practice in providing regulatory, legal, and technology solutions to law firms, legal publishers, and in-house law departments around the world, overseeing our team of experienced US attorneys and data and technology experts. Will has over 25 years' experience working with corporations to improve the management of their legal and corporate compliance functions. Will began his legal career as a litigator with a predecessor firm to Drinker, Biddle LLP. He then served as in-house counsel to Andersen Consulting LLP, managing risk and working with outside counsel on active litigation involving the firm.

Will has leveraged his legal experience interpreting regulations and appearing before federal (DOJ, SEC, FTC) and state agencies (NYAG) to oversee research and other areas at Bear Stearns. In this capacity, he counseled analysts on regulatory risk and evolving compliance requirements. Will also consulted on the development of a proprietary tool to ensure effective documentation of compliance clearance of research reports. Will then went on to work in product development and content creation for a global online compliance development firm pioneering the dynamic updating of regulated firms' policies and procedures from online updates and resources. Will holds a Juris Doctorate with High Honors from the Washington University School of Law in Saint Louis and is admitted to state and federal bars. He lives in Pawling, NY, with his wife and daughter.

Sanjay Sharma, PhD
FOUNDER AND CHAIRMAN

Pranav Menon, Esq.
LEGAL RECRUITMENT MANAGER AND DATA PRIVACY SPECIALIST – LAW & COMPLIANCE | GPESR

GreenPoint> Law&Compliance

About GreenPoint Law & Compliance

- GreenPoint Global was founded in 2001 and since that time has faithfully served an expanding roster of clients. GreenPoint leverages a unique combination of US-trained attorneys and proprietary technology to deliver a unique offering of skill and flexibility to meet client needs.
- Our core team of experienced US attorneys is based in Israel and works US hours. The breadth of experience of our attorneys ensures high-quality, cost-effective results across a wide range of legal, compliance, and regulatory matters.
- GreenPoint's methodology and proven track record of achieving client objectives has resulted in a broad base of clients in the United States, ranging from Fortune 500 insurance companies to solo practitioners, law firms, in-house law departments, and legal publishers. GreenPoint attorneys are selectively recruited and deployed based on possessing demonstrable subject matter expertise covering a broad spectrum of substantive US laws and regulations. The work product of our attorneys is thoroughly vetted internally before delivery to client. Adherence to quality, value and flexibility is at the core of our foundation.

GreenPoint> Global

About GreenPoint Global

- GreenPoint Global provides litigation support, finance and technology solutions to insurers, law firms, banks, and in-house law departments through our subject matter experts and process specialists.
- Founded in 2001 and headquartered in Rye, New York, GreenPoint has grown to over 500 employees with a global footprint. We have a stable and growing client base that ranges from small and medium-sized organizations to Fortune 1000 companies worldwide. Our production and management teams are located in the US, India, and Israel with access to deep pools of subject matter experts. Our greatest strength is our employee-base of experienced lawyers, paralegals, process specialists, financial analysts, and software developers. We have leading edge software development capabilities with over 50 professionals on staff, working on internal and client projects.
- GreenPoint is certified by the TÜV SÜD (South Asia) for the highest standards of Quality Management (ISO 9001:2015) and Information Security Management (ISO 27001:2013). GreenPoint is certified as a Minority and Woman Owned Business Enterprise (MWBE) by New York City and a Minority Owned Business Enterprise (MBE) by the State of New York. GreenPoint complies with all federal and state contracting requirements. GreenPoint is owned by its founders and principals and is debt free. For comprehensive information on our services and products under Law & Compliance and Finance, please visit our subsidiary websites through the division's menu.