JS|HELD

PERSPECTIVES

Off-Channel Communications: How Financial Services Organizations Can Address Regulators' Latest Target

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

As a number of recent headlines demonstrate, the U.S. Securities and Exchange Commission (SEC) and other regulators have fined and penalized employers and employees in the financial services industry for non-compliance with regulations related to off-channel communications (OCC). Off-channel communications occur when employees use unapproved and inadequately protected devices – such as personal cellphones – or applications to communicate with co-workers, counterparties and / or clients. Many financial services firms are required to maintain copies of all communications regarding their business, supervise the same, and produce them in response to regulatory requests. Firms cannot meet those compliance obligations when employees resort to unauthorized OCC for business-related matters.

In charging 15 broker-dealers and one affiliated investment advisor in September 2022 with record-keeping violations, the SEC noted that its investigation uncovered employees at all levels of these firms who routinely used text messaging apps on their personal devices to discuss business matters between January 2018 and September 2021.[1] The firms settled the charges and agreed to pay penalties totaling more than $1.1 billion. Just as important, the firms also agreed to engage independent compliance consultants to ensure the use of OCC meets regulatory standards as part of the settlements.

In a related move,[2] the Commodity Futures Trading Commission (CFTC) ordered 11 financial institutions to pay more than $710 million for recordkeeping and supervision failures for widespread use of unapproved communication methods such as personal texts, WhatsApp, and Signal. Additionally, the Financial Industry Regulatory Authority (FINRA) has also taken action when it comes to OCC.

In addition to guaranteeing that these communications are properly documented and retained, the regulations are set up to prevent the use of OCC to manipulate securities transactions or commit fraud and to ensure that it is not used to violate any other securities laws. Firms' supervisory procedures must be reasonably designed to detect for OCC when they monitor for such activity.

By implementing effective processes and utilizing software and outside experts to monitor and detect OCC, broker-dealers, investment advisers, and other financial institutions can reduce the risk of regulatory enforcement and penalties and ensure that they remain in compliance with regulations. This article discusses the risks that OCC pose for financial services firms, especially as the SEC, FINRA, and the CFTC have made it clear that they are now targeting firms throughout the industry about their OCC to see if they are recording and preserving business information according to regulations. The authors also explain how firms, including broker-dealers of all sizes, should manage their OCC to ensure that they and their employees comply with federal securities laws and regulations. Finally, the authors address the complexity related to the collection of OCC in response to regulatory enforcement investigative requests. As the fines and settlements between those firms and the SEC exemplify, financial services firms of all sizes need to take this regulatory focus seriously and take the proactive step of engaging an independent third-party with expertise and experience in both digital forensics and compliance issues.

Risks, Pitfalls, and Mitigation When Implementing OCC Controls

The SEC has made clear in its examination priorities – as seen in the excerpt below – that it will be scrutinizing OCC and what firms are doing about these communications to stay in compliance.[3]

V. BROKER-DEALER AND EXCHANGE EXAMINATION PROGRAM

A. Broker-Dealers

The Division has long emphasized the importance of robust broker-dealer compliance and supervisory programs as a proactive measure to ensure compliance with the federal securities laws. This year, the Division intends to focus examinations on broker-dealer compliance and supervisory programs generally, including those for electronic communications related to firm business, as well as the recordkeeping for those electronic communications.

DID YOU KNOW?

The Division intends to focus examinations on broker-dealer compliance and supervisory programs generally, including those for electronic communications related to firm business, as well as the recordkeeping for those electronic communications.

[1] https://www.sec.gov/news/press-release/2022-174
[2] https://www.cftc.gov/PressRoom/PressReleases/8599-22
[2] https://www.sec.gov/files/2023-exam-priorities.pdf P. 17

While some financial institutions mitigate risk by providing business devices to employees to use for all business communications, this may not be cost effective or feasible for many firms. In addition, OCC concerns are still present as clients and counterparties may still use the employees' personal devices for communicating. These risks involve:

- **Security:** Personal devices may not have the same level of security as company-issued devices, making them more vulnerable to cyberattacks and data breaches.
- **Compliance:** Use of personal devices may not comply with regulations and industry standards, such as those regarding record-keeping and data protection.
- **Privacy:** Employees may store sensitive company information on their personal devices, which may not be properly secured or erased if the device is lost or replaced.

To mitigate these risks, financial institutions can work with outside experts to implement policies and procedures for secure BYOD (Bring Your Own Device) usage, such as implementing strong passwords, encryption, and remote wipe capabilities. Digital forensics experts can also work with organizations to perform defensible data preservation of mobile devices or select chat applications to ensure client-related communications are securely captured while maintaining employee confidentiality and privacy. They can also conduct regular security audits and staff training to ensure compliance with industry standards and regulations.

In addition, companies can use specialized software and mobile device management (MDM) solutions to monitor and secure the use of personal devices for work purposes, supplement, and bolster keyword supervisory controls, and provide technical support and guidance to employees.

However, even with these safeguards in place, there are still some potential pitfalls associated with OCC. These may include:

- Lack of documentation or retention of communications, and a lack of proper oversight or supervision of off-channel communications,
- Lack of focused training emphasizing management priority and clearly worded employee attestations,
- Inadequate supervisory and workflow controls, end-to-end,
- Loss of context when communications are captured in part or are incomplete,
- Lack of transparency by employees in complying or providing all communications,
- Improper or partial presentation or production of OCC content to regulatory agencies.

Software for OCC Compliance

There are several software applications available to help financial institutions manage OCC, including:

- Compliance management systems - These systems allow financial institutions to monitor and track OCC and ensure that they are compliant with regulatory requirements.
- Email archiving systems - These systems help firms store and organize emails and other electronic communications for easy access and review.
- Electronic Communications Management (ECM) Tools - ECM tools automate the process of capturing, storing, and tracking OCC, reducing the risk of lost or missing information.
- Mobile communication monitoring systems - These systems track and monitor OCC that occur via mobile devices, such as text messages or chat applications.

However, these tools have some limitations, including:

- Incomplete data capture - Some systems may not capture all off-channel communications (either due to software limitations or inadvertent omissions by employees), leading to gaps in the records.
- Lack of integration with existing systems - Integrating OCC management tools with existing systems can be challenging, leading to errors or incomplete data.
- Lack of customization, indexing, robust / complex keyword searching or production offerings.

- Cost - Implementing and maintaining these tools can be expensive.

Expertise Needed to Improve OCC Management

Financial institutions may benefit from outside guidance for two main reasons. First, by improving its overall OCC posture and ensuring that all OCC communications are properly managed and recorded. This can involve training for employees on how to handle OCC and the development of policies and procedures to manage these communications to minimize risk and increase efficacy of compliance protocols. Second, consulting services can help an organization respond to a preservation / collection effort, which generally is an enforcement request for all OCC for a specific period. In particular there are privacy concerns when dealing with personal information on all employees BYOD devices especially key employees who often are the target of the requests. Also, sophisticated analytical tools may provide the basis to reduce OCC messages that truly are not business communications.

Digital forensics and compliance experts can also assist financial institutions in reviewing and evaluating their current methods and software applications for handling OCC. They can provide a comprehensive analysis of the firm's current processes, including a review of their software tools and systems for preserving, storing, searching, and tracking OCC. Limitations of these tools can be identified, such as the inability to fully index entire threads or capture communications that occur outside the confines of the software. Otherwise, experts can be directly involved in the workflow to ensure a defensible and compliant end-to-end process utilizing bespoke as well as industry-recognized forensic and discovery tools.

CONCLUSION

With more employees working remotely and regulatory agencies taking a tougher approach to OCC, financial services firms need to make sure their business communications and data governance policies are updated and enforced so that they are complying with recordkeeping and supervision regulations.

Utilizing an independent third-party may provide comfort to senior management and / or regulators that a sufficient arms-length overview of a firm's communications program was conducted. In particular it can address privacy concerns when collecting OCC for regulatory requests. By engaging outside experts, firms – including broker-dealers and investment advisers – can better understand the regulatory requirements and ensure that all OCC is properly documented, in compliance with regulations, and adequate measures are in place to manage the risks associated with OCC.

Firms need to clearly state their OCC policy to employees and make them aware of the privacy and data breach risks that can occur through the use of personal devices and unauthorized messaging platforms. Furthermore, employees should be made aware of the obligations the firms have to preserve and maintain books and records as well as monitor internal communications such as emails and messages, in order for those communications to be made readily available for requests from regulators.

The SEC has made it clear that other broker-dealers and investment advisers who are subject to similar recordkeeping and supervision regulations should scrutinize their internal controls and correct any deficiencies. Compliance consultants with expertise in digital forensics can help firms of any size perform comprehensive analyses of their policies and procedures on the retention of communications found on employees' personal devices and unauthorized messaging apps. By conducting these reviews, financial services firms can meet this new target of regulators head-on and with confidence.

Acknowledgements

The authors would like to thank Mike Gaudet and Omer Khan for providing additional insight and expertise.

Antonio Rega is a Managing Director in J.S. Held's Digital Investigations & Discovery group within the Global Investigations Practice. He has more than 20 years of experience providing consulting, advisory, and subject matter expertise in the areas of digital forensics, data privacy & information governance, digital assets / blockchain technology and discovery on behalf of global corporations and law firms. Based in New York, Antonio focuses on leading complex investigations and matters involving proactive and

reactive discovery and analysis, often conducting in-depth forensic examinations of electronically stored information (ESI) across repositories (cloud-based, localized, or mobile). He regularly assists clients with advisory and strategy through all phases of investigations, regulatory compliance or litigation needs, such as privacy-related regulatory requests, responses to government subpoenas, and related information governance needs, among other areas of specialization.

Prior to joining J.S. Held, Antonio led large-scale investigations and compliance matters involving digital forensics, data privacy and eDiscovery at several leading consultancies. He has served as a guest lecturer at Fordham University School of Law on the topic of data privacy and related technology. He also contributes material and discussion as a content editor for the American Bar Association (ABA), as well as participating as a member of the Sedona Conference Trade Secrets Working Group 12.

Antonio is a Certified Fraud Examiner (CFE); EnCase Certified Examiner (EnCE); Computer Certified Examiner (CCE); Cryptocurrency Tracing Certified Examiner (CTCE), CipherTrace; Blockchain Council's Certified Cryptocurrency Auditor (CCA); TRM Labs Certified Investigator (TRM-CI); and Licensed Private Investigator (PI) for the State of Texas.

Antonio can be reached at antonio.rega@jsheld.com or + 1 551 3345 8592.

John Ivan is a Managing Director in J.S. Held's Financial Services group within the Global Investigations Practice. He is a securities industry attorney and compliance professional who has led both compliance and legal departments for major financial institutions, with a focus on wealth management, brokerage and advisory issues including a wide array of SEC - and FINRA- related regulatory matters. In a previous role, he served as Chief Compliance Officer for Raymond James & Associates, Inc., the full-service retail, and capital markets broker-dealer based in St Petersburg, Florida, and was Head of Compliance for all of Raymond James' retail and dual registrant businesses. Prior to that, he was Managing Director at Bank of America Merrill Lynch covering compliance for its Global Wealth and Retirement Services products and services business. Previously, he was General Counsel and Chief Compliance Officer for Janney Montgomery Scott LLC, in Philadelphia, and held the Series 7, 8, 14, 24, 63, and 65 security industry licenses. John also served in senior compliance and legal roles at Goldman Sachs in New York, and at Wells Fargo Advisors' predecessor firms.

John can be reached at jivan@jsheld.com or +1 224 263 7822.

Stephen Strombelline is a Managing Director in J.S. Held's Financial Services group within the Global Investigations Practice. He has more than 35 years of compliance and regulatory experience, along with enterprise risk management credentials within the securities and banking industries. In a previous role, he was Head of Corporate Compliance for Charles Schwab Corp. Stephen began his career at the NASD (now FINRA), where he was appointed as Associate Director of the New York District office. He later served as Chief Compliance Officer in the United States for Barclays Capital and BNP Paribas. He has served as Chairman of the National Society of Compliance Professionals (NSCP) and the Institute of International Bankers' Compliance Committee and was an Executive Committee Member of SIFMA's Compliance & Legal Society.

Stephen can be reached at sstrombelline@jsheld.com or +1 224 263 7835.

More About J.S. Held's Contributors

Mike Gaudet is a Managing Director in J.S. Held's Digital Investigations & Discovery group within the Global Investigations Practice. He has more than 20 years of experience providing solutions for corporations, legal teams, and government agencies related to data discovery and governance challenges. He is an expert eDiscovery practitioner and technologist, with a master's in computer science. He has proficiency in leveraging the right tools to quickly gain insight from data, and to efficiently achieve project goals on time and under budget. He has experience executing ad-hoc projects as well as designing and implementing Software-as-a-Services (SaaS) solutions.

Mike can be reached at mike.gaudet@jsheld.com or +1 281 415 5742.

Omer Khan is a Managing Director in J.S. Held's Digital Investigations & Discovery group within the Global Investigations Practice. Omer specializes in designing, developing, and implementing the organization's applications

development and systems analysis function with a special focus on financial crime prevention, anti-money laundering, sanctions, and regulatory matters affecting banks, custodians, gaming companies, and foreign banks. Prior to joining J.S. Held, he held leadership positions at several major high-tech and financial companies with projects that span the globe. His expertise includes data science & machine learning; data integration & governance; automation engineering; model validation, tuning, and testing; software development; project management, crypto currency, anti-money laundering; sanctions, fraud compliance programs; and Know Your Customer (KYC) due diligence.

Omer can be reached at omer.khan@jsheld.com or +1 845 317 7989.