WHITE COLLAR WATCH

BLANKROME

APRIL 2018 • NO. 1

CONTENTS

Note from the Editors

Welcome to the spring edition of our *White Collar Watch.* Hopefully by the time you are reading this, winter's storms (finally?) are behind us.

2018 has gotten off to a busy start for our practice and attorneys. We look forward to continuing to work with our clients on understanding new regulations and assessing trends that may affect their companies and industries, and stand ready to assist when and as needed.

In this edition, we serve up a white collar alphabet soup, with pieces on **AML, e-ORBs, FCA, FCPA,** and **MVRA:** how FinTech companies can mitigate their risk of exposure to regulatory enforcement actions by ensuring compliance with anti-money laundering laws; the maritime industry's increasing use of electronic oil-record books to improve the monitoring of shipboard environmental compliance; the likelihood that False Claim Act *qui tam* cases may increase following a new Department of Justice memorandum issued this past January; the increasing scrutiny of hiring practices of financial institutions with respect to Asian markets; and a pending U.S. Supreme Court case involving a circuit court split over whether the mandatory restitution statute requires restitution for the costs of client's internal investigations.

We hope you enjoy this edition, and welcome any feedback.

JOSEPH G. POLUKA
PARTNER

INBAL P. GARRITY
PARTNER

WILLIAM B. SHIELDS
OF COUNSEL

EDITORS, *WHITE COLLAR WATCH*

Client Investigative Expenses: Reimbursable as Restitution, or Not?

BY JOSEPH G. POLUKA, MARK M. LEE, AND HUAOU YAN

JOSEPH G. POLUKA
PARTNER

MARK M. LEE
PARTNER

HUAOU YAN
ASSOCIATE

On January 12, 2018, the U.S. Supreme Court granted *certiorari* in *Lagos v. United States,* 864 F.3d 320 (5th Cir. 2017), *cert. granted,* 138 S. Ct. 734 (U.S. Jan. 12, 2018), to resolve a persisting circuit split over whether the Mandatory Victims Restitution Act ("MVRA") requires restitution for the costs of internal investigations and attorneys' fees incurred separately and independently from the government's official investigation.

Background

In *Lagos,* defendant-petitioner Sergio F. Lagos pleaded guilty to one count of conspiracy to commit wire fraud and to five counts of wire fraud, arising from a revolving-loan financing agreement between Lagos (and his company USA Dry Van Logistics LLC) and General Electric Capital Corporation ("GECC"). Specifically, GECC extended financing to Lagos based upon the value of his company's accounts receivable. In order to secure increased financing, Lagos and his co-conspirators falsified their accounts receivable to the tune of $26.726 million by, *inter alia,* recording fictitious sales and "paying" the company for those fictitious sales with some of the money borrowed from GECC.

> The D.C. Circuit's and Judge Higginson's narrower reading of § 3663A(b)(4) is the minority position. Counting the Fifth Circuit, seven of the eight circuits that have considered the question have taken the broader view of that statutory provision.

District Court Ruling

The U.S. District Court for the Southern District of Texas sentenced Lagos to 97 months of imprisonment and three years of supervised release. The court also ordered restitution pursuant to the MVRA, and Lagos agreed that he was responsible to GECC, the victim, for the money he still owed GECC under the financing agreement, totaling about $11 million. However, Lagos disagreed with the court that he was liable under the MVRA for an additional $4.895 million to compensate GECC for forensic expert fees, legal fees, and consulting fees. GECC incurred those expenses conducting an internal investigation of Lagos' fraud and in participating in USA Dry Van Logistics' bankruptcy proceedings.

The crux of the dispute revolves around the meaning of 18 U.S.C. § 3663A(b)(4), which requires (for certain crimes) restitution for "lost income and necessary child care, transportation, *and other expenses incurred during participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense.*" (Emphasis added.)

Lagos contends that the plain language of this clause is applicable only to *necessary* expenses incurred by a party *participating* in the *official government criminal investigation and prosecution.* Thus, an internal investigation undertaken outside of the government's official investigation and "neither required nor requested"[1] by the government—as in his own case—is simply not covered by the statute. In opposition, the government contends that Lagos' unreasonably narrow interpretation fails to comport with the MVRA's substantive purpose of ensuring that victims of a crime receive full restitution.

The Fifth Circuit Weighs In

In a brief opinion, the Fifth Circuit upheld the district court's restitution award. Based on prior Fifth Circuit cases that had given a broad reading to § 3663A(b)(4), the Fifth Circuit found that GECC's internal investigatory and legal costs—which were caused directly by Lagos' fraud—easily fell within the scope of that statutory provision.

The Concurrence

Although he concurred with the judgment of the court, Judge Stephen A. Higginson separately wrote to suggest that the Fifth Circuit may be interpreting § 3663A(b)(4) too broadly. Judge Higginson first expressed his agreement with the D.C. Circuit's "persuasive interpretation" of the statute in *United States v. Papagno,* 639 F.3d 1093 (D.C. Cir. 2011). In *Papagno,* the D.C. Circuit held that, as a matter of straightforward statutory interpretation, costs incurred through an internal investigation neither required nor requested by the government are not covered by the § 3663A(b)(4). As a preliminary matter, the D.C. Circuit noted that the singular "offense" referred to in the section is the criminal offense of conviction, and the singular "investigation or prosecution" is the official criminal investigation and prosecution conducted by the government. The D.C. Circuit then focused on the term "participation," finding that it has a narrower meaning than "assistance"—*i.e.,* that an internal investigation may have *assisted* the government's investigation does not mean that the internal investigators participated in the government's investigation. The D.C. Circuit also highlighted § 3663A(b)(4)'s use of the term "necessary," which further militates against its application to such an internal investigation—an internal investigation neither required nor requested by government investigators is by definition "unnecessary."

Judge Higginson then noted three additional points that further support the D.C. Circuit's narrower reading of the statute: 1) Breaking the statute down, Judge Higginson read § 3663A(b)(4) to allow reimbursement for a victim's participation in the investigation of the offense, participation in the prosecution of the offense, and attendance at proceedings related to the offense. In his view, because the latter two can occur only within the context of the government's criminal enforcement, that implies that the first—participation in the investigation of the offense—must also be limited to the context of the government's criminal enforcement; 2) the Fifth Circuit's broad interpretation may be difficult to administer, requiring district courts to determine the scope of "the investigation" and what expenses were "necessary"; and 3) limiting the reach of § 3663A(b)(4) does not prevent victims from fully recovering their losses. Other criminal restitution provisions may allow recovery, and even where they fall short, victims may bring their own civil actions.

Final Thoughts

The D.C. Circuit's and Judge Higginson's narrower reading of § 3663A(b)(4) is the minority position. Counting the Fifth Circuit, seven of the eight circuits that have considered the question have taken the broader view of that statutory provision.[2] We shall see what the court has to say. □

1. Petition for a Writ of Certiorari, *Lagos v. United States,* No. 16-1519, 2017 WL 2665926, at *I (U.S. June 15, 2017).

2. *See, e.g., United States v. Janosko,* 642 F.3d 40, 42 (1st Cir. 2011); *United States v. Amato,* 540 F.3d 153, 159-60 (2d Cir. 2008); *United States v. Elson,* 577 F.3d 713, 727-28 (6th Cir. 2009); *United States v. Hosking,* 567 F.3d 329, 332 (7th Cir. 2009); *United States v. Stennis-Williams,* 557 F.3d 927, 930 (8th Cir. 2009); *United States v. Nosal,* 844 F.3d 1024, 1046-47 (9th Cir. 2016).

The FinTech Revolution: Complying with Anti-Money Laundering Laws to Avoid Regulatory Enforcement Actions

BY BRIDGET MAYER BRIGGS AND ARIEL S. GLASNER

BRIDGET MAYER BRIGGS
ASSOCIATE

ARIEL S. GLASNER
ASSOCIATE

This is the fourth installment in a series of articles. For more background on this topic, please read our first article in the series, An Introduction to Financial Technology; our second article, The FinTech Revolution: Enforcement Actions Brought against FinTech Companies and Their Implications; and our third article, The FinTech Revolution: The Impact of Blockchain Technology on Regulatory Enforcement.

As we recently highlighted, financial technology ("FinTech") companies are attracting increasing attention from financial services regulators, owing in part to the proliferation of criminal actors who utilize FinTech companies to perpetrate frauds. In this article, we examine how companies can best minimize the risk of exposure to a regulatory enforcement action by ensuring their compliance with applicable Anti-Money Laundering ("AML") laws.

> FinTech companies must have an effective AML program in place when they begin offering financial services or products to avoid exposure to a regulatory enforcement action.

BSA Compliance

The Bank Secrecy Act ("BSA"), 31 U.S.C. § 5311, *et seq.,* was enacted to help root out criminal activity occurring within the banking system. Under the BSA and the implementing regulations promulgated by the Financial Crimes Enforcement Network ("FinCEN"), "financial institutions" are required to establish AML programs and to verify the identities of account holders through "Know Your Customer," or "KYC," provisions.[1]

Many FinTech companies squarely meet the definition of a "financial institution" under the BSA, as it includes banks, money services businesses ("MSBs"), brokers and dealers in securities, mutual funds, insurance companies, operators of credit card systems, and loan or finance companies.[2] This definition covers, for example, peer-to-peer transfer systems (such as Venmo) and digital wallets (such as Google Wallet). FinTech companies that are not financial institutions may still be obligated to adhere to the BSA to have access to banks in order to promote their financial services. Indeed, many banks that originate loans or process payments on behalf of FinTech companies require them to have detailed AML compliance policies in place as part of the bank's own KYC program.

Congressional Activity

In March of this year, FinCEN published a letter to the U.S. Senate Finance Committee setting forth its position that companies that sell virtual currencies, including through token sales such as Initial Coin Offerings ("ICOs"), must comply with AML requirements. Congress has further signaled to FinTech companies that may consider themselves beyond the BSA's reach, including issuers or exchangers of digital currencies, to not get too comfortable. Toward the end of 2017, the Senate Judiciary Committee held a hearing to consider proposed Senate Bill 1241, which would expand the definition of a financial institution to include "[a]n issuer, redeemer, or cashier of prepaid access devices, digital currency, or any digital exchanger or tumbler of digital currency."

Compliance with the BSA requires financial institutions to, among other things: 1) maintain an adequate AML and KYC program; 2) file Currency Transaction Reports ("CTRs") for transactions over $10,000; 3) file Suspicious Activity Reports ("SARs") when the institution "knows, suspects, or has reason

to suspect that the transaction (or a pattern of transactions of which the transaction is a part)" involves money laundering, is designed to evade the requirements of the BSA, serves no apparent lawful purpose, or facilitates criminal activity; and 4) register with the Department of Treasury.[3]

The Legal Consequences of Noncompliance

Many FinTech companies, especially startups, are more focused on developing their products and services rather than dedicating scarce resources to develop and implement compliance programs. However, the BSA does not exempt fledgling companies from its scope. FinTech companies must have an effective AML program in place when they begin offering financial services or products to avoid exposure to a regulatory enforcement action. Failure to have a comprehensive AML compliance program in place can expose FinTech companies to other potential civil or criminal liability under the Racketeer Influenced Corrupt Organizations Act; the Financial Institutions Reform, Recovery, and Enforcement Act; the Anti-Fraud Injunction Statute; or the Federal Trade Commission Act.

FinTech companies must be aware of how the BSA applies to their business so that they can implement appropriate AML programs to reduce their legal exposure and avoid facilitating illicit activities. Given the complexities of this area of law and the risks associated with potential enforcement actions, FinTech companies should consult with legal counsel to develop a compliance program that will address all potential business lines. ◘

1. 31 U.S.C. § 5318(h), (l); 31 C.F.R. § 1010.200 ("Each financial institution (as defined in 31 U.S.C. § 5312(a)(2) or (c)(1)) should refer to Subpart B of its Chapter X Part for any additional program requirements…").
2. 31 C.F.R. § 1010.200, *et seq.*
3. 31 C.F.R. §§ 1022.210; 1022.310; 1022.320; 1022.380; 1023.

Financial Institutions' Hiring Practices under the Microscope: The Importance of Anti-Corruption Programs

BY SHAWN M. WRIGHT, MAYLING C. BLANCO, AND RICHARD WOLF

SHAWN M. WRIGHT
PARTNER

MAYLING C. BLANCO
PARTNER

RICHARD WOLF
ASSOCIATE

On February 14, 2018, another major financial institution disclosed that it is under investigation for possible violations of the Foreign Corrupt Practices Act ("FCPA"). This disclosure comes at a time when the Department of Justice ("DOJ") and the Securities and Exchange Commission ("SEC") continue to scrutinize the hiring practices of financial institutions in and with respect to their Asian markets.

Investigations of Financial Institutions Operating in Asia

In its earnings statement, the financial institution announced that the DOJ and the SEC are investigating its "hiring practices in the Asia Pacific region and, in particular, whether [it] hired referrals from government agencies and other state-owned entities in exchange for investment banking business and/or regulatory approvals" in violation of the FCPA.[1] In November 2016, a similar financial institution and its Hong Kong-based subsidiary agreed to pay the SEC, the DOJ, and the Federal Reserve Board $264 million to settle charges that it violated the FCPA by hiring unqualified employees referred by government officials, particularly those with connections to upcoming transactions.[2] Other financial institutions have been investigated for similar practices in the region.[3]

The DOJ and the SEC apparently have uncovered well-established corrupt patterns and practices in the region and are planning to investigate or are already investigating others for similar misconduct, possibly aided by recently recruited cooperators in the region and the industry. Financial institutions operating abroad, especially in Asia, need to scrutinize their current and past hiring in light of these developments to identify any FCPA exposure, implement corrective measures, and make necessary disclosures.

Preventing Violations

The FCPA prohibits U.S. financial institutions and those with securities listed on U.S. exchanges from making any corrupt payment or offering anything of value to a foreign official for the purpose of obtaining or retaining business, or gaining any improper advantage. Hiring a friend or family member of a government official as a favor or a form of persuasion to

secure a contract, business, permit approvals, or other favorable treatment violates the FCPA. Hiring interns referred by or related to government officials may be common in certain foreign countries and even may be viewed as a "cost of doing business abroad." However, under the FCPA, these practices are unlawful and can carry hefty fines; cultural norms, also known as "everybody does it," are no defense.

Hiring interns referred by or related to government officials may be common in certain foreign countries and even may be viewed as a "cost of doing business abroad." However, under the FCPA, these practices are unlawful and can carry hefty fines; cultural norms, also known as "everybody does it," are no defense.

Financial institutions can protect themselves by developing and enforcing a strong anti-corruption and detection program that includes clear policies and procedures for compliance with the FCPA, comprehensive FCPA training programs for managers and those responsible for hiring, and a process for ensuring that due diligence is performed for new hires.

Remediating Violations

If a financial institution suspects that its hiring practices (or other conduct) violate the FCPA, then corrective measures must be taken promptly. First, it should investigate to determine if a violation occurred and, if so, its nature and extent. Second, remediation likely will require clearer policies and procedures, stronger internal controls, additional training, and disciplinary action against the employees involved. Finally, the financial institution must consider whether it should voluntarily self-disclose the issue to the DOJ. Self-disclosure of FCPA violations is not mandatory, but given the recent heightened scrutiny and increased prosecutorial activity, the significant benefits of self-disclosure, whether through the traditional route or via the Pilot Program,[4] must be given careful consideration.

Understanding the present enforcement landscape and what can be done to avoid as well as remedy common pitfalls is key for companies operating in high-risk regions where these practices may be historically embedded in the industry. □ –

1. *Friday Roundup,* FCPA Professor (Feb. 16, 2018), available at http://fcpaprofessor.com/friday-roundup-239.
2. *SEC Enforcement Actions: FCPA Cases,* U.S. Securities & Exchange Comm'n, sec.gov/spotlight/fcpa/fcpa-cases.shtml (last accessed Mar. 20, 2018).
3. Erika Kelton, *US Accelerates Pursuit of Companies for FCPA Violations,* Forbes (Dec. 23, 2016), available at forbes.com/sites/erikakelton/2016/12/23/us-accelerates-pursuit-of-companies-for-fcpa-violations/#3f1c827050b0.
4. Carlos Ortiz, Shawn Wright, Mayling Blanco & Ariel Glasner, "The Benefits of Corporate Anti-Corruption Programs: No Charges," *White Collar Watch* (Dec. 2017) at 8-9, available at blankrome.com/sites/default/files/2018-01/WhiteCollarWatch-12-2017.pdf.

Notable Industry Events & Presentations

Upcoming

BLANKROME

Webinar

Blockchain and Cryptocurrency Litigation Concerns: Class Actions, Criminal Exposure, and Criminal Tax Implications

Wednesday, April 11 • 1:00–2:00 p.m. (EDT)

Online via WebEx

Click here to register

Blockchain technology and cryptocurrencies are not only dominating the headlines, they're changing the way companies do business. As the regulatory, transactional, and litigation landscapes continue to evolve at a rapid pace, Blank Rome's attorneys have maintained cutting-edge knowledge of the issues facing a broad range of businesses in a wide range of areas.

This seminar will cover some of the most important issues facing companies today, including:

- Blockchain basics—what you need to know
- White collar issues surrounding the adoption of blockchain applications or the use of digital currencies, including SEC, CFTC, state enforcement efforts, and criminal tax implications
- Class action vulnerabilities and implications

PRESENTERS

Michelle Gitlitz
Partner
Financial Services

Carlos Ortiz
Partner & Chair
White Collar Defense and Investigations

Ana Tagvoryan
Partner
Business Litigation

Shawn Wright
Partner & Chair
White Collar Defense and Investigations

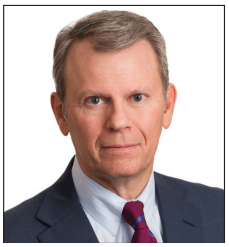
Please contact Marianne Talbot for more information about this event.

Recent

- **Ariel S. Glasner** presented a CLE on Understanding and Analyzing the SEC Investigative Report on Initial Coin Offerings for Lorman Education Services (March 29, 2018).
- **Mayling C. Blanco** served as a panel member for BITCOINS & BLOCKCHAINS & CRYPTOTECHS, OH MY! Demystifying the World of Virtual Currency and Distributed Ledger Technology, and Understanding How They Are Changing the World as We Know It at the 2018 Hispanic National Bar Association Corporate Counsel Conference & Moot Court Competition (March 16, 2018).
- **Gregory F. Linsin** presented on MARPOL Security Agreements: Past Time for the U.S. Coast Guard to Remedy Abuse at the Connecticut Maritime Association's 2018 Shipping Conference (March 14, 2018).
- **Joseph G. Poluka** presented on the topic of Enforcement at the American Conference Institute's 31st FDA Boot Camp (March 9, 2018).

False Hope for False Claims Act Defendants? Government Dismissals of *Qui Tam* Cases May Increase

BY NICHOLAS C. HARBIST AND LAUREN E. O'DONNELL



NICHOLAS C. HARBIST
PARTNER

LAUREN O'DONNELL
ASSOCIATE

On January 10, 2018, the Department of Justice ("DOJ") Civil Fraud Section Director, Michael Granston, sent an internal memorandum (the "Memorandum") to attorneys responsible for civil False Claims Act ("FCA") enforcement. The Memorandum provides guidance to DOJ attorneys considering whether to dismiss FCA *qui tam* cases. The Memorandum begins by noting that, while the number of FCA *qui tam* cases has increased substantially over the years, the rate of government intervention has remained the same. The Memorandum advises DOJ attorneys to consider seeking dismissal as they evaluate whether to intervene.

The Memorandum

The Memorandum's introduction notes that the government expends significant resources in *qui tam* cases, even when the government declines to intervene because it monitors non-intervened cases and is sometimes required to produce discovery or otherwise participate in the proceeding. The introduction observes that cases that lack substantial merit can generate adverse decisions that affect the government's ability to enforce the FCA. Thus, according to the Memorandum, dismissal is an important tool to advance the government's interests, preserve limited resources, and avoid adverse precedent. Given this backdrop, the Memorandum appears to be encouraging DOJ attorneys to consider dismissing more cases initiated by private relators.

SEVEN FACTORS

The Memorandum identifies seven factors, which are neither mutually exclusive nor exhaustive, to consider:

1. Is the legal theory defective and/or are the factual allegations frivolous?
2. Does the action duplicate a pre-existing government investigation without providing additional useful information?
3. Has the relevant government agency determined that the action threatens to interfere with the agency's policies or programs?
4. Is dismissal necessary to protect DOJ's litigation prerogatives because the action, for example, adds to excessive lawsuits or could result in unfavorable precedent?
5. Will dismissal help safeguard classified information?
6. Are the costs of litigation likely to exceed any expected gain?
7. Does the relator's action frustrate the government's effort to investigate because, for example, the relator has failed to provide all material information to the government?

ADDITIONAL POINTS

The Memorandum concludes with several points. Notably, it reminds DOJ attorneys that they need not dismiss the entire case; they can dismiss certain claims or defendants to streamline a matter. It also encourages DOJ attorneys to advise relators of perceived deficiencies in their cases, as well as the prospect of dismissal, so that relators can consider dismissing the action on their own.

The Road Ahead

Some commentators have cautioned that defense counsel should manage their expectations about the Memorandum because 1) it largely reflects a restatement of longstanding considerations and legal provisions regarding FCA dismissals, and 2) the DOJ may continue to seek dismissal only in rare circumstances. The fact that the government reported $3.7 billion in FCA recoveries in settlements and judgments in 2017 makes some commentators skeptical that the DOJ will bite the hand that feeds it by dismissing more cases.

At the very least, the Memorandum provides a roadmap for how defense lawyers can frame motion practice, government presentations, and discovery to entice the DOJ to consider dismissal. Defense counsel should thus be mindful of the Memorandum and lobby the DOJ to dismiss cases accordingly. □

Environmental Compliance Aboard Commercial Ships: Electronic Recordkeeping Is Overdue

BY GREGORY F. LINSIN AND KIERSTAN L. CARLSON

GREGORY F. LINSIN
PARTNER

KIERSTAN CARLSON
ASSOCIATE

U.S. environmental laws impose substantial recordkeeping and reporting obligations on regulated industries. The Environmental Protection Agency ("EPA") and state agencies use these records to monitor compliance and evaluate the need for enforcement actions. Historically, the EPA resisted transitioning to electronic recordkeeping for environmental compliance data due to concerns about the reliability and security of electronic reporting. Recently, however, the EPA moved fully to electronic recordkeeping, compliance reporting, and data sharing, which allows regulated entities to identify and address potential violations through more streamlined reporting and monitoring.

Despite these advances for land-based industries, little has been done to modernize environmental recordkeeping and reporting requirements for the maritime industry. The principal maritime environmental treaty, MARPOL,[1] requires commercial ships to maintain logbooks to verify compliance with numerous operational and environmental requirements. MARPOL and its implementing U.S. statute and regulations require ships to document all transfers and discharges of oily waste in a hard-copy Oil Record Book ("ORB"), which must be available on demand for inspection by the U.S. Coast Guard.

Any intentional errors or omissions in an ORB can lead to federal criminal prosecution on false records charges under MARPOL or 18 U.S.C. § 1001. The Department of Justice ("DOJ") prosecutes 10–15 criminal MARPOL enforcement cases each year, nearly all of which charge at least one false ORB count. These prosecutions can result in criminal fines and/or imprisonment of top-ranking ship officers.

Most maritime companies comply with MARPOL requirements because they are committed to responsible stewardship of the marine environment; the financial and reputational consequences of a MARPOL violation can be crippling. Yet, companies struggle with compliance because of the challenge of maintaining real-time oversight of ships that trade all over the globe.

Trend toward E-ORBs

The maritime industry is trending towards the use of electronic ORBs, which will improve companies' ability to monitor shipboard environmental compliance. Led primarily by Liberia, several flag administrations now authorize ships sailing under their flags to use "e-ORBs."

Collectively, these authorizations require data preservation and verification, retention of printed copies of e-ORB entries for a certain time period, and use of pre-approved e-ORB software. E-ORBs *will* provide a number of operational benefits, including the ability of shoreside personnel to detect discrepancies in log entries in near real-time, thus enabling companies to correct or mitigate potential noncompliant operations and potentially avoid an enforcement action.

The International Maritime Organization ("IMO") expects to issue formal guidance and amendments to MARPOL on the use of e-ORBs and other MARPOL logbooks by 2019. The IMO's Marine Environment Protection Committee ("MEPC") has developed draft "Guidance for the Use of Electronic Record Books under MARPOL," which addresses compliance considerations for e-ORBs, such as 1) security and verification of entries; 2) data storage and preservation; and 3) the need for e-ORB software to meet company audit requirements. Moreover, the MEPC's Sub-Committee on Pollution Prevention and Response ("PPR") has considered the feasibility of transitioning to electronic MARPOL record books, and is finalizing the non-mandatory guidelines and developing draft amendments to MARPOL that will permit the use of electronic record books.

It is regrettable that, instead of taking the lead at the IMO to modernize recordkeeping aboard commercial ships in a way that will enhance environmental compliance, the United States is dragging its anchor.

There is near-uniform support for the move to electronic record books, but the United States is a holdout, expressing concern about the "safety, security, protection, and availability" of electronic logbooks, and about allowing countries to accept electronic logbooks prior to formal amendments to MARPOL. It is regrettable that, instead of taking the lead at the IMO to modernize recordkeeping aboard commercial ships in a way that will enhance environmental compliance, the United States is dragging its anchor.

E-ORBs as a Compliance Mechanism

Despite the United States' position, maritime companies can increase MARPOL compliance simply by utilizing e-ORB software and transitioning other ship records to an electronic format. By doing so, companies can monitor and analyze ORB entries in real-time, rather than waiting for periodic shipboard audits. The real-time verification of ORB entries by shoreside technical staff, especially when coupled with the review of other key data, such as tank sounding records, will improve shipboard compliance and help companies more readily detect and address noncompliance. It also will assist companies in determining whether a voluntary disclosure is needed, which, in turn, will facilitate cooperation between companies and regulators, and reduce enforcement risks for responsible companies.□ – ©2018 BLANK ROME LLP

This article was first published in Mainbrace (March 2018), Blank Rome's quarterly maritime newsletter.

1. MARPOL refers to the International Convention for the Prevention of Pollution from Ships, as modified by the Protocol of 1978. It was developed by the International Maritime Organization ("IMO") to address various forms of pollution, including discharges of oil, air emissions, and garbage dumping.