Guidepost

# FOCUS ON FOREIGN BANKS' SANCTIONS COMPLIANCE PROGRAMS IN THE U.S. AND GLOBALLY *UPGRADING AND EMPOWERING COMPLIANCE TO HELP ADDRESS NATIONAL SECURITY RISKS*

As the Russia – Ukraine war rages on, one outcome so far is clear: the Western nations remain aligned and united to confront Russian aggression. The West's synchronized, roll-out of economic and trade sanctions against Russia since February 2022 combined with their limited military support, demonstrate that the West's tight, global coordination helps Ukraine courageously defend its nation and citizens. Importantly, coordinated alignment also protects the homeland and critical infrastructure of each Western nation, including that of the United States.

Banks and financial institutions are essential participants of and in effect, combatants of the Russia – Ukraine war. They must therefore be fully equipped and empowered to meet the needs of all sanctions and other legal and regulatory requirements. The war to combat terrorism, money laundering, sanctions evasion, bribery, corruption, cybercrimes, and fraud of course, has been waged beyond Russia, and long before February 2022.

**The Big Picture:**

Foreign banks operating in the United States ("FBOs") through their U.S. branches, agencies, and subsidiaries and other "U.S. persons"[1], must rigorously comply with all sanctions. This includes sanctions against Russian government and targeted individuals and oligarchs, and others such as Iran, North Korea, Cuba, and thousands of their agents. This is especially true for rules enforced by the U.S. Treasury Office of Foreign Assets Controls ("OFAC"), U.S. Commerce, and

State Departments, and prosecuted by the U.S. Department of Justice ("DoJ").

It is therefore essential and time-critical that FBOs review and refresh their anti-financial crime, cybersecurity, as well as enterprise-wide compliance risk management programs, now. To do so, FBOs and their group headquarters must be fully aligned, including having an empowered and adequately resourced chief compliance officer and compliance program at both the U.S. regional and group head office levels.

Just as the West's finance ministers and regulators are aligned and coordinated to minimize the weakest link, so too must FBOs and their home office.

**Why It Matters:**

The risks and therefore, stakes are huge for FBOs and other "U.S. persons." Violating the continuously changing and multiple sanctions, AML, cyber, crypto, and other global rules can be reputationally damaging and costly. Indeed, breach of these rules can also result in a threat to the national security of U.S., European, Japanese, Australian and other western nations.

The consequences can be therefore, catastrophic. Keeping pace with and complying with the ever-changing list of sanctions, AML, cyber, crypto, "CFIUS"[2], and other global rules are not mutually exclusive either. Internal controls must be strong to combat each and every one of these risks holistically.

**Additional Challenges for Foreign Banks in the U.S.**

FBOs operating in the United States are especially vulnerable. This is because they are equally accountable and liable for sanctions violations however large or small their size and nature of their U.S. offices and business activities. FBOs are even more vulnerable if they must depend heavily on their home office technologies – and culture of compliance (or lack thereof), which might not meet the West's strict and continuously changing sanctions and other compulsory legal and regulatory compliance expectations.

Additionally, although the Western sanctions are coordinated and aligned, they are not identical. Exceptions exist within each country particularly relating to the energy sectors. FBOs whose headquarters are based in Europe, Australia, Japan, and the U.S. must therefore comply with each of these nuanced differences with robust compliance IT algorithms, effective operational processes and the right quantity and quality of skilled compliance teams.

**Non-Alignment with the West**

Not all nations participate in the West's sanctions against Russia either. This poses a compliance dilemma for FBOs headquartered in Asian, Latin American, African, and the Middle Eastern nations which are not participating ("nonparticipating nations"). On the one hand, FBOs operating in the U.S. must comply fully with each of the West's Russia (and other) sanctions in the U.S. and wherever they operate in the West; on the other hand, they must comply

with the geopolitical objectives of their home countries' non-participation.

### "Sanctions Are the New FCPA," and Chief Compliance Officer Liability & Certifications

Given the threat to the United States' and West's national security interests, the DoJ, OFAC, and other U.S. and international regulators intend to heavily enforce the sanctions compliance requirements. The DoJ also seeks to empower chief compliance officers ("CCOs") to help companies including FBOs, comply with these complex requirements.

This is because the DoJ recognizes the key role that CCOs and compliance functions play to address the significant sanctions, financial, and national security risks to the "essential critical" infrastructure of the U.S. and the West. These include telecommunications, food, healthcare, technology, energy, and other key sectors – especially with the financial services sector as the global payments "backbone" across these industries.

One area of relative success by the DoJ and U.S. Securities and Exchange Commission ("SEC") has been the U.S. extraterritorial reach and international cooperation to combat bribery and corruption through enforcement of the U.S. Foreign Corrupt Practices Act, or "FCPA." The DoJ and U.S. government also recognize that sanctions evasion is a major and real risk. This is because of the harsh reality that cybercrime, use of cryptocurrencies and other digital assets, money laundering, terrorist finance, and bribery and corruption are not mutually exclusive. And with so many "non-participating nations," the risks of sanctions evasion are magnified. Consequently, the DoJ has: 1) armed Federal prosecutors with greater enforcement powers, 2) targeted a greater number of individuals including senior executives through enforcement, 3) sought to empower CCOs by requiring joint compliance certifications by the chief executive and chief compliance officer, and 4) proclaimed that "sanctions are the new FCPA", given the reach and relative success of the FCPA as a template to strengthen sanctions compliance.

### CCO Certifications Can Help Map Out Processes, Controls and Reinforce Accountability

Despite an industry-wide buzz over the DoJ's pronounced intent to require CCO *and CEO* compliance certifications after a company remediates a criminal resolution, firms including FBOs should embrace the certification process to proactively strengthen their sanctions and enterprise compliance programs[3]. This is because the DoJ view certifications as a means to empower CCOs while improving the corporate compliance culture. Certifications compel firms including FBOs to map out their compliance processes and underlying controls, and foster accountability of business, operational and other executives so they are held accountable for the controls for which they are responsible.

The New York State Department of Financial Services ("DFS") already requires NY state supervised institutions to certify their compliance with cyber security and AML- and sanctions compliance requirements. It is an excellent means (whether regulated by the DFS or not) to identify and remediate compliance and control processes and most importantly, to align culture and compliance accountability through sub-certifications rolling up to CEO and CCO

certifications.

**Key Takeaways for FBOs (and Other Foreign Companies Operating in the U.S.)**

Violating the U.S. and the West's sanctions compliance requirements can be catastrophic on multiple fronts. If the West's global regulators are aligned and communicating regularly with one another, so must your FBO's U.S. CCO with his / her home country compliance counterparts. They must regularly communicate and align to consistently comply with the complex and ever-changing sanctions requirements.

If you are an FBO (or any other "U.S. person"), you must review and refresh your sanctions, anti-money laundering, bribery and corruption and overall enterprise compliance risk management program, now.

Our team of sanctions and enterprise compliance experts can assist your business in navigating the constantly changing rules and regulations that impact your compliance and reputational risk management program. We stay up to date on the latest nuances of preparation and remediation processes and procedures through active and on-going engagements with small, medium, and large, complex FBOs and other U.S. persons impacted by the West's sanctions against Russia and other targeted nations, entities, and individuals. Our team regularly provides highly informative and interactive training to personnel charged with sanctions and other compliance responsibilities. Sanctions risk is a significant issue with multiple potential downsides to all U.S. businesses. We are here to help you minimize that risk across the sanctions and broader, enterprise compliance spectrum.

[1] Per OFAC and Commerce Department, "U.S. persons" includes: 1) all U.S. citizens and permanent resident aliens regardless of where they are located; 2) all persons and entities within the United States (including U.S. offices of foreign companies including FBOs), and 3) all U.S. incorporated entities (e.g., JP Morgan) and their foreign branches. and other

[2] The Committee on Foreign Investment in the United States ("CFIUS")

[3] The Sky Will Not Fall with New Justice Department CEO / CCO Certifications; Instead, the Sun Will Shine – Guidepost Solutions


## ERIC YOUNG

Senior Managing Director


Eric T. Young advises highly regulated organizations on reengineering compliance, ethics, and regulatory technology programs to enable reputable and sustainable business growth. He has deep regulatory experience having spent close to 40 years in chief compliance officer roles at some of the world's largest institutions, including five global banks.

Throughout his career, Mr. Young has remediated and transformed corporate compliance programs and financial crime compliance programs including sanctions; integrated compliance and ethics cultures between regions, countries and companies to ensure consistency across enterprises; built compliance budgets; enhanced reporting; created governance frameworks and risk assessment, monitoring and testing programs; closed compliance gaps; restructured compliance teams; and mentored junior staff to create a pipeline of future compliance leaders and enable grassroots compliance ideas, solutions and digital upgrades.