




## Sanctions compliance and enforcement in Asia: understanding the implications

Sanctions are used to pressure a country or regime into changing their behavior and to prevent terrorist financing. At a time when regulators in the Asia-Pacific region are stepping up their sanctions enforcement and monitoring, many financial institutions are still laboring under a misconception: that simple technical compliance is an adequate response to the United Nations (UN) and United States (U.S.) sanctions impositions.

In reality, regulators in China, Hong Kong and Singapore are increasingly focused on robust programs defined by the legal obligations and risk profiles of the institution under scrutiny—particularly on the role played in detecting and reporting financial crime. More and more, regulators are demanding that institutions go beyond UN and Office of Foreign Asset Control (OFAC) lists to develop their own proprietary lists. These may include additions such as ISIS foreign fighters or extended 50% ownership of sanction entities. Moreover, these regulators have bolstered their expectations for executing sanction controls through their investment in additional staff and in sanctions screening and training.




The result is that noncompliant financial organizations are finding themselves subject to millions of dollars in fines imposed to achieve maximum deterrence. And the worst consequences of enforcement action go beyond the fines. Reputational damage can be immeasurable, and reacting to an enforcement action often saps an organization's financial strength. Compliance enforcements can be costly due to the loss of business during the investigation and remediation process. It can frequently lead to loss of leadership where it can cost upwards of \$3 million to replace a key senior executive. In addition, acquiring outside counsel and consultants to defend against the claim can cost \$1,000 per hour.

Add in the cost of development and implementation of compliance systems—between \$2 million and \$500 million per project according to industry experts—and the picture becomes clear: these types of issues can easily cripple a company for years, or even put it out of business.

## The trend is toward more sanctions supervision and enforcement with higher penalties

Under the current U.S. administration, significant changes were made to many sanctions programs, including a new policy course on Cuba sanctions and a bolstering of OFAC administrative sanctions against hostile countries such as Iran, North Korea and Syria.

The U.S. ceased to participate in the Joint Comprehensive Plan of Action (JCPOA) and began re-imposing economic and trade sanctions in Iran. Additionally, an OFAC advisory is in effect to alert companies to deceptive shipping practices used by North Korea to evade sanctions, requiring parties subject to monitoring U.S. and/or UN sanctions to implement appropriate controls to ensure compliance. The longstanding Syria sanctions program—one of the most comprehensive sanctions programs currently administered by OFAC—remains in effect as a result of the ongoing violence and human rights abuses taking place in Syria.



There is no doubt about the seriousness with which U.S. authorities are enforcing these sanctions. There has been more than one sanctions action per week in 2017 and 2018 and billions of dollars of fines levied by OFAC. In the latest of a string of regulatory probes or fines by U.S. regulators, a few high-profile cases stand out:

**ICBC Case:** In May 2018 Industrial and Commercial Bank of China Financial Services, a Chinese multinational bank, was fined U.S. \$5.3 million to settle charges by the Financial Industry Regulatory Authority.<sup>1</sup> It was determined that the bank did not have adequate anti-money laundering systems in place to monitor and detect suspicious transactions. Analysts predict that the actions will likely slow its overseas markets growth.

**ZTE Case:** In March 2017 the leading Chinese telecom equipment manufacturer was fined a record-high combined civil and criminal penalty of U.S. \$1.19 billion against Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd. for selling telecommunications equipment to Iran and North Korea in violation of U.S. sanctions and export controls.<sup>2</sup> A seven-year blockade was imposed by Washington.


These cases are just the tip of the iceberg. In 2018, regulators are focusing more on evolving vulnerabilities resulting from the rapid pace of technological change. Both the U.S. and EU are now viewing the absence of a robust compliance program as an aggravating factor when a violation is determined, resulting in higher penalties. Even low transaction values are not immune to OFAC scrutiny.

## Shifts of enforcement are already taking place

As more and more companies find themselves in OFAC's crosshairs, there have been shifts in enforcement by regulators notably in Singapore and Hong Kong, including sanctions as part of compliance reviews. With an international peer review of its AML compliance requirements on tap for 2019, Japan's Financial Services Agency is urging financial institutions to do a better job with CDD/KYC and suspicious transactions.<sup>3</sup> India is also taking a cue from the global community as anti-bribery and anti-corruption enforcement has seen significant traction in the past few years.<sup>4</sup>

## It is now imperative to control the impact of sanctions expectations

There is no doubt that managing escalating sanctions requirements in a rapidly evolving Asia-Pacific economy while balancing the realities of operations and budget constraints is a complex challenge. It is now evident that organizations must take deliberate steps to implement and maintain a sanctions compliance program that will meet regulatory expectations.



**Increasing workflow efficiency with access to comprehensive and current sanctions lists is a key way to support the evolving requirements of risk-based strategies. With seamless access to authoritative, global financial crime intelligence, organizations can synchronize screening, increase operational efficiencies, mitigate the impact of global volatility and meet complex compliance expectations.**

LexisNexis® Bridger Insight® XG, seamlessly integrated with WorldCompliance™ Data, is the portal to aggregates of sanctions and enforcement information from the most important sanction lists (OFAC, EU, UN, BOE, FBI, Bureau of Industry and Security and more). In addition, it contains information received from enforcement lists and court filings worldwide, such as the FDA, U.S., HHS, UK FSA and SEC.

By applying these due diligence practices, your organization can help avoid the staggering legal costs and months of notoriety associated with sanctions violations and position itself as a compliant leader.

**For more information, visit [risk.lexisnexis.com/BIXG-EN](http://risk.lexisnexis.com/BIXG-EN)**



### About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit [www.risk.lexisnexis.com](http://www.risk.lexisnexis.com) and [www.relx.com](http://www.relx.com).

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

<sup>1</sup> <http://www.finra.org/newsroom/2018/finra-fines-icbcfs-53-million-anti-money-laundering-compliance-deficiencies-and-other>

<sup>2</sup> <https://www.nytimes.com/2017/03/07/technology/zte-china-fine.html>

<sup>3</sup> <http://www.amlpartners.com/news/aml-compliance/fatf-review-japan-aml-compliance/>

<sup>4</sup> <http://www.forbesindia.com/blog/business-strategy/india-catching-up-on-international-trends-on-compliance/>

Bridger Insight XG and WorldCompliance Data provided by LexisNexis are not provided by “consumer reporting agencies” as that term is defined in the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) (“FCRA”) and do not constitute a “consumer report” as that term is defined in the FCRA. Bridger Insight XG and WorldCompliance Data may not be used in whole or in part as a factor in determining eligibility for credit, insurance, or employment or for any other eligibility purpose that would qualify it as a consumer report under the FCRA. Due to the nature and origin of public record information, the public records and commercially available data sources used in reports may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. This product or service aggregates and reports data, as provided by the public records and commercially available data sources, and is not the source of the data, nor is it a comprehensive compilation of the data. Before relying on any data, it should be independently verified. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. WorldCompliance is a trademark of World Compliance Inc. Bridger Insight is a registered trademark of LexisNexis Risk Solutions Inc. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2018 LexisNexis. All rights reserved. NXR12422-00-0418-EN-US