Thomson Reuters MENA Market Insights

Eradicating your supply chain of sanctions and reputational risk

The recent U.S. sanctions case against ZTE Corp. has underscored the importance of a robust sanctions risk management strategy that reaches into every tier of an organization's supply chain. This investigation, which resulted in record-setting penalties, threatened the reputation of several high-profile technology brands that supply ZTE Corp, including Qualcomm, Microsoft and Intel.

ZTE Corp., which includes China's Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd., has agreed to a combined civil and criminal penalty of USD 1.19 billion, pending consent from the courts. This eye-watering fine – the largest ever imposed by the U.S. government in an export control case – was levied after ZTE Corp. was investigated for evading U.S. sanctions and export control laws governing the shipping of equipment to Iran and North Korea.[1]

As part of the settlement, ZTE Corp. will pay a penalty of USD 661 million to the U.S. Bureau of Industry and Security (BIS), with USD 300 million suspended during a seven-year probationary period.

Supply chain impact

ZTE's Chief Executive has released a statement that the organization "acknowledges the mistakes it made, takes responsibility for them, and remains committed to positive change in the company". However, ZTE Corp. is still subject to a seven-year suspended denial of export privileges, which could be triggered if there are further violations.

This means that the group's U.S. supplier base – which provides 25-30% of its components and includes Qualcomm, Microsoft and Intel – remains at risk of revenue loss, given the possibility that their trade arrangements with ZTE Corp. could be affected if the export ban is activated.

The importance of managing supply chain risk

Like many other corporations around the world, companies in the Middle East and North Africa (MENA) region with exposure to complex supply chains are putting robust sanctions and reputational risk management strategies into place.

It can be a constant challenge to ensure compliance with all the sanctions requirements imposed by different governments, especially since their targeted entities vary and these are frequently updated. However, considering the potentially devastating consequences of being associated with a sanctions breach – even inadvertently – it's crucial to keep pace with sanctions developments. It's also necessary to have a clear view on all the risks that your organization is vulnerable to on every tier of your supply chain.

Failure to comply with sanctions requirements, export controls and other regulatory expectations can have severe repercussions for your organization on many levels. A compliance breach can involve weighty fines and even criminal penalties (depending on the case), it can also cause reputational damage that takes years to patch up and smooth over – especially when your end users are ethically-minded millennials.

How to protect your organization against sanctions and reputational risk

- **Establish an enterprise-wide strategy for risk control**
  In many cases, it is not the complexity of the supply chain or sanctions landscape that exposes companies to risk, but rather a lack of a cohesive approach to monitoring suppliers from the beginning of the supply chain through to the end user. While it is important for the risk management and compliance functions to work independently from the internal audit team and C-suite to avoid conflicts of interest, it is essential to maintain synergies between these departments. Each of these functions play a crucial role in the risk management process and if they're operating in silos and not communicating with each other, this could lead to gaps in risk coverage.
- **Follow a continuous risk-based approach (RBA)**
  An effective way to manage sanctions risks and other risks inherent in multiple business relationships is to adhere to a continuous RBA process. Ideally, this involves assessing the entire supply chain, identifying the vulnerabilities that the company is exposed to, establishing a clear plan for mitigating these risks, and continuously monitoring and evaluating this plan and its implementation.
- **Implement a routine screening process**
  Screening a supplier at the onboarding stage is just the beginning of an effective Know Your Supplier (KYS) process. Circumstances can change at any time; and it's essential to implement routine screening of all existing suppliers and partners against a database of strictly monitored risk intelligence on individuals and entities globally. What if one of your suppliers has been added to a sanction or watch list, or been linked to an investigation into unlawful conduct after you've already onboarded them?
- **Undertake enhanced due diligence**
  For high risk parties, organisations can use an enhanced due diligence platform that provides more extensive screening and background checks on any entity or individual in any location. Sometimes, it is essential to look beyond sanctions lists and to build a more detailed picture of your supplier, searching for adverse media and hidden risks in business relationships and human networks.

Navigating the evolving risk landscape

One lesson learned from the ZTE scandal is that regulators are clamping down more aggressively than ever on organizations that violate sanctions and export controls. While ZTE Corp. is still afloat, not all companies are in the position to handle the financial burden of paying such steep penalties – or the reputational fall-out that comes with such a high-profile scandal.

In this environment, organizations with global distribution networks and multi-tiered supply chains need to take a rigorous, ordered and strategic approach to mitigating the sanctions and compliance risks that they may be exposed to through vendors, sub-contractors, suppliers or even end users.

This may require incorporating sophisticated screening technologies and intelligence tools into your KYS and enhanced due diligence processes. It may also involve implementing an organization-wide risk culture that creates a sense of accountability for sanctions and reputational risk management from the boardroom through to the business units – and across the risk, compliance, internal audit and supply chain management functions.

David Shepherd
Market Development Lead for Risk
Thomson Reuters MENA

David Shepherd is the Market Development Lead – Risk (Middle East & North Africa) at Thomson Reuters and is responsible for developing the market strategy for the Thomson Reuters Risk Division in MENA.

He holds a Diploma in Financial Crime and Compliance and brings over 10 years experience in Risk, specialising in areas such as Ultimate Beneficial Ownership, Adverse Media, Sanctions and Watch List Data as well as legislation including FCPA, UK Bribery Act and global AML and KYC standards.

David has extensive market experience having worked with prominent Financial Institutions, Governments and Multinational Companies both in Europe and across the Middle East and North Africa. He has been based in MENA in the Dubai Head Office since joining Thomson Reuters in 2013.

1 https://commerce.gov/news/press-releases/2017/03/secretary-commerce-wilbur-l-ross-jr-announces-119-billion-penalty

2 http://indianexpress.com/article/technology/tech-news-technology/chinas-zte-pleads-guilty-settles-us-sanctions-case-for-nearly-900-million/

For more information about Thomson Reuters risk management solutions, please visit mena.thomsonreuters.com/en/corporate-solutions-mena/risk-management.html