We are now Refinitiv, formerly the Financial and Risk business of Thomson Reuters. We’ve set a bold course for the future – both ours and yours – and are introducing our new brand to the world.

As our brand migration will be gradual, you will see traces of our past through documentation, videos, and digital platforms.

Thank you for joining us on our brand journey.
The expansion of economic sanctions has meant financial institutions are increasingly expected to adopt and implement a sophisticated “risk-based” approach to compliance. This is especially the case given the strict criminal liability nature of sanctions offences and “zero tolerance” approach taken by relevant competent authorities and enforcement agencies.

Asset freezing restrictions under EU and UK financial sanctions regimes prohibit both dealing with the funds or economic resources (a concept which is widely defined in sanctions legislation to cover any asset which may be used to obtain funds, goods or services) of a sanctions target (a designated person) and making funds or economic resources available directly or indirectly, to or for the benefit of, a designated person.

A critical question for any financial institution and its legal/compliance team is therefore how it both ensures that it is not doing business with a designated person or an entity which is owned or controlled by a designated person and how it manages its third party risk i.e. a third parties with which it does business diverting its products or services to a designated person or an entity which is owned or controlled by a designated person.

WHAT IS SANCTIONS SCREENING

The international framework for financial sanctions does not proscribe the processes which financial institutions need to adopt in relation to sanctions compliance. Nor do relevant competent authorities, including the UK HM Treasury, generally publish any guidance on “de minimis” levels for sanctions screening. Financial institutions are expected however to adopt and maintain appropriate “risk-based” policies and procedures to ensure compliance with their legal obligations.

International sanctions regimes require absolute compliance and any person in breach of a legal obligation will be guilty of an offence, unless a successful defence is established. The only defence available under current EU sanctions regulation is that a company did not know and had no reasonable cause to suspect that its actions would violate international sanctions obligations.

The nature of international sanctions legislation means that a company risks breaching its sanctions obligations as soon as any new individual or entity is “designated” and listed under the relevant sanctions regime. Relevant competent authorities expect financial institutions to take a proportionate response to compliance with their sanctions requirements. As such, financial institutions are expected to implement appropriate systems and procedures to identify persons who are subject to financial sanctions, based on the company’s assessment of the likelihood of dealing with such persons and the associated risk of breaching its sanctions related obligations.

A RISK-BASED APPROACH

Financial institutions should take an approach to sanctions screening which is appropriate for their business model when assessing where, when and how their business is most likely to encounter designated persons, and focus resources and tailor systems and controls accordingly.

Financial institutions, particularly those with many different client types, product types and/or geographical markets, should consider carrying out an assessment in order to be able to understand which parts of their business may carry a greater exposure to sanctions risk.

In particular, a company should focus enhanced counterparty diligence and screening exercises on areas of the company’s business that carry a greater likelihood of involvement with sanctions targets, or their agents, for example:

• Entities incorporated, registered, headquartered or domiciled in, or which are known to operates in, any jurisdiction that is subject to an international sanctions regime (remember however that a designated person may be incorporated or operating in a jurisdiction that is not subject to an international sanctions regime);
• Entities incorporated, registered, headquartered or domiciled in or which are known to operates in any wider sensitive destination for financial crime risk (e.g. Middle East, Eastern Europe, Turkey); or
• Where there is reasonable cause to suspect that any counterparty derives its profits from activities prohibited under international sanctions measures.

PRACTICAL TIPS

• Screening is only as good as the inputted data — some financial institutions find that they have gaps or inconsistencies in their data e.g., data from a long term client whose data was not fully captured or data stored across disparate systems. Effort in the short term to ensure a complete and coherent data set reduces the risk of missing a potential match during the screening process or identifying a number of “false positives” i.e. the identification of an apparent match to a designated person which is assessed on investigation not to relate to a sanctions target.

Continued
EXPERT TALK: SANCTIONS COMPLIANCE: THE IMPORTANCE OF SCREENING

• It is important to consider “fuzzy matching”, as names might be missed if only exact matches are screened. “Fuzzy matching” describes any process that identifies non-exact matches. Where a firm uses a screening system which has a fuzzy matching capability, it should ensure that the fuzzy matching process is calibrated as appropriate in line with the risk profile of their business.

• Many individuals who are on sanctions lists intentionally attempt to obscure their identities to avoid detection. These individuals may alter the spelling of their name, which parts of their name they use, or alter other facts such as date of birth. For this reason financial institutions may wish to consider whether their screening tools can screen using several protocols — e.g., name reversal, number removal, number replaced by word, etc.

• As part of a wider risk assessment exercise, financial institutions should consider the frequency of sanctions screening for existing clients.

• A comprehensive sanctions screening policy will need to consider who reviews potential sanctions matches from the screening process, what training they have and how often it is repeated and how sanctions hits are escalated within the business.

• Financial institutions should keep a written record of their screening policy and be able to justify the timescales and frequency of screening, resolution of screening matches and regulatory reporting if required.

• Consider other ways of risk mitigation: As an added layer of risk management, and in addition to sanctions screening, consideration should be given to what sanctions-related protections (e.g. specific representations and warranties) are included in the company’s contractual agreements with its counterparties and to manage third-party risk.

Finally, appropriate sanctions screening should form part of a wider process of risk assessment, identification and management which also includes:

1. an appropriate level of understanding of international sanctions regimes;
2. the implementation of procedures and training programmes;
3. the screening of transactions (in order to identify and manage “activity-based” restrictions); and
4. wider reporting of matches and voluntary self-disclosure of violations of sanctions related obligations.

AUTHOR BIO:

John Forrest is a partner. He regularly counsels clients on the handling and coordination of multijurisdictional investigations involving alleged violations of international sanctions, export controls and customs regulations.

Chloe Barker advises clients on international trade, investment and regulatory issues, particularly sanctions, export control, anti-dumping and wider import/customs regulation. The views expressed are her own.

First published in Thomson Reuters Regulatory Intelligence on 6 July 2015

RISK MANAGEMENT SOLUTIONS FROM THOMSON REUTERS
Risk Management Solutions bring together trusted regulatory, customer and pricing data, intuitive software and expert insight and services – an unrivaled combination in the industry that empowers professionals and enterprises to confidently anticipate and act on risks – and make smarter decisions that accelerate business performance.

For more information, contact your representative or visit us online at risk.thomsonreuters.com