Getting all your ducks in a row

March 2023

The environment for winning and retaining business has rarely been more challenging. Most prominently, in geo-political terms, the Russian invasion of Ukraine and the knock-on effects on politics and economies worldwide. In addition, the rising tensions between China and Taiwan, an escalated war of words and ideology between various delineations of 'East' and 'West', and the cost-of-living crisis arguably replacing coronavirus as the number one cause of economic panic.

A long-drawn-out pandemic, followed immediately by global instability and economic turbulence has left, once more, trustworthy companies acting far less diligently, partly perhaps, because they are so desperate for business and are prepared to pay the price. But why take the risk?

Businesses that could not openly work with Russia were forced, in an already difficult environment, to look elsewhere. To do so with confidence, when the alternative providers of oil & gas are nations such as Venezuela, Saudi Arabia, and Iran (all marketplaces as corrupt as Russia), is an added onus.

In Know Your Customer (KYC) and 'client comfort' terms, if a deal with Rosneft and its mafia-backed elite is the frying pan, Venezuela's Petróleos de Venezuela S.A (PDVSA) is very much the fire.

The alternative was for companies to seek loopholes or shortcuts in Russia's sanctions program and claim that their particular individual or corporate entity was clean and therefore fine to work with, even if this is self-evidently untrue.

Look closely and Russia's war in Ukraine has changed everything, and nothing. Everything, because Russia has become *patriam non grata* as sanctions officially prevent Western businesses from partnering with them. Nothing, because Russia has been the sick man on the fringes of Europe for years, and sanctions have always been circumvented or ignored in the past.

More recently however, on more than one occasion, KCS Group Europe has been asked to conduct due diligence to approve corporate entities connected to the notorious oligarch, Mikhail Friedman, on the basis that he does not directly own the companies, therefore the client would not be directly working for a sanctioned figure. This is a) semantics and b) wilfully ignoring the point of due diligence in the first place.

Alternatively, many UK law firms are looking to work with Yandex, the Russian search engine and technology firm, despite the sanctions applied against its founder, Arkady Volozh, and the company's role as a pro-Kremlin mouthpiece. In both these cases, the impetus seems to be "*find us a way where we can work with these companies*", and implicit in the request is the admission that this is inappropriate.

This also works the other way: a Russia affected by broader and deeper sanctions is taking a more global approach to its business, making increased use of second and third-hand networks to transfer monies and ship products in contravention of sanctions, and relying on international partners who are either complicit or naïve enough to work with them.

A number of American technology firms are using Turkish companies to sell products to Russian entities, with little evidence that KYC is being conducted to ensure that their actions are not contravening sanctions. It's a point highlighted by the fact that calling the Turkish entities 'companies' is charitable, when they are shells and cut-outs designed to facilitate transfers with no awkward questions being asked.

The same is true of shipping firms in Greece selling oil believed to originate from Russia, before disappearing as quickly as they were created. Deception and obfuscation have always been key elements in the Russian playbook – but Moscow is being assisted enormously by the inadequacies of Western due diligence and compliance or the desire not to know the truth.

It is, of course, not only Russia that is triggering a divesting of compliance norms. The global economic uncertainty has made the race for growing markets – particularly those in Africa and the Middle East – tighter and nastier and, to some extent, businesses are taking off their gloves and doing whatever they feel they need to do to survive. But if ignoring KYC in some of the most dangerous and challenging markets on the planet is foolish, wilfully turning a blind eye is borderline insane. And yet, it is evident that lawyers, accountants, and bankers alike are attempting to 'find a way' to do business with entities that they know are unsuitable, either because they are so desperate for business in the current dire economic straits or because their only concern is to bring the money in regardless of the cost down the line. The consequences of this will be severe: fines at best, disbarments, and criminal investigations at worst.

Yet the short-termism persists, not only in the act of pursuing unsuitable clients in the first place but in the practice of how the KYC checks are done. In-house compliance analysts tend to rely on freely available social media and databases to make their calls, when such a limited source base is inadequate because of the degree to which bad actors are already manipulating online information, or because the databases can only tell you what is already known and not what lengths the target may have gone through to hide. Even the framing of KYC itself is being diminished, with increasing requests to target only certain aspects of criminality or consider a facet or locality as off-limits.

In some cases, monitoring these types of individuals with their varied ways of manipulating online profiles is not easy. Cases are emerging of individuals who have a fair amount of information on them available through open sources but are restricted to basic facts. Similarly challenging are cases when there is hardly any information on an individual at all which, although more likely to raise alarm bells, fail to enable an informed decision to be made on whether they are, in fact, clean.

This highlights a need to rethink how conclusions are made from a basic due diligence check. There is a need to step back and ask why? Does the individual's background based on nationality and economic status alone raise alarm bells? If so, why does open-source information on them not add up with this?

KCS Group Europe has observed a group of Russian businessmen using both information manipulation and elimination tactics online. The need for deeper dive due diligence should not be restricted to desktop searches alone. Instead, by considering the numerous risks that come with an entity's geopolitical and economic background, you begin to see the need to go beyond an initial level of screening and, in turn, unravel the multi-layered *matryshkas* (Russian dolls) of individuals whose online profiles give impressions that are otherwise too good to be true.

In other cases, it is hard to ignore the impression that – as illustrated with Yandex and Friedman - clients do not want to look too closely because they already fear what may be found. Meanwhile, there may be no acknowledgement or direction on the issue at board level because directors, according to those with current knowledge of the sector, are primarily concerned only with preventing cyber-attacks in the heightened Russia-fuelled threat climate, or are invested in the short-term money themselves, on the basis that this makes their immediate position and remuneration stronger and any problems will be someone else's to deal with.

So let us offer some predictions. The deterioration in quality, and quantity, of compliance and KYC will decrease in inverse proportion to its growing necessity. The ‘cost-cutting’ approach instituted during the coronavirus pandemic, where deep due diligence by expert outside firms was relegated in favour of cheaper in-house operations, will continue - but this time be driven more by a desire to better control the information and the consequences. The Solicitors Regulation Authority and Financial Conduct Authority will compile ever-longer lists of sensitive cases where the profit motive outweighs the moral or legal actualities. And a ‘perfect storm’ will come at some point, where the short-term attitude of firms, the disinterest of directors, and the inadequacies of how KYC is enacted will all coalesce into a situation that sees a major legal or financial firm publicly and expensively humiliated. They may well deserve it.

It is high time for companies to reconsider their KYC practices or lack thereof, and to make the commitment to focus on a new approach to compliance that puts properly conducted, enforceable due diligence at the heart of corporate decision-making. These practices should not be bound by profit motive or outside influence and must be viewed as a contributing factor to a company’s success rather than a distraction from it.

After all, best practice KYC and due diligence will enhance rather than hinder your business, and most importantly protect your interests from international reputational damage.

KCS Group Europe - Strategic Intelligence & Corporate Security

A leading provider of security and intelligence services, we operate discreetly in some of the world’s most difficult environments on complex cases of fraud, theft, corruption, or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients identify and deal with any risks, weaknesses and threats which could impact on their business, financially or reputationally.

Our key areas of expertise include:

Corporate Intelligence Services - New market or sector entry research - Know your customer screening.

In addition, we offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits - providing unparalleled analysis, contingency planning, and implementation.

To find out more or to arrange a meeting to discuss your business needs, please email the team at info@kcsgroupeurope.com or call (00 44) 2072451191.

www.kcsgroup.com