





Navigating the global sanctions landscape in 2022

Sanctions compliance in an era of rising global tensions

Pressure resulting from geopolitical shifts ensures that governments will continue to rely on sanctions as a critical tool in exercising economic power and pushing their policy goals.

The global sanctions landscape in 2022

The expansive use of sanctions as a tool to achieve policy goals shows no sign of abating. The US, EU, UK and many other countries continue to make sanctions central to many foreign policy challenges. Pressure brought on by both near- and longer-term geopolitical shifts ensures that governments will continue to rely on sanctions as a critical tool in exercising economic power and pushing their policy goals.

In the latest edition of our biennial report, Navigating the global sanctions landscape, we look at some of today's most critical sanctions compliance challenges—from country and regional issues to concerns around cryptocurrency, ransomware, and transaction and third-party risk.

A mix of change and continuity from the US

At just over a year into the Biden administration, sanctions legislation has become more targeted, less open to legal challenge, and to an extent, easier to apply and interpret. We've seen a shift back to multilateral coordination and an increase in dialogue around mitigating the unintended economic and political impacts of sanctions, particularly for humanitarian actors. But at the time of writing in February 2022, the most significant changes to country regimes were the measures adopted against Russia and Belarus.

Geopolitics increasingly key to EU sanctions policy

The EU is another key source of sanctions policy, and to a lesser extent, enforcement. Despite the perennial challenge of political consensus, the EU is increasingly using sanctions as a policy tool of first resort in most major international crises, with member states showing a willingness to absorb the economic costs. The relatively new European Commission has tried to assert Europe's independent geo-economic power, using sanctions more frequently as a deterrent rather Russia is a remarkable case in point.

The EU is also using sanctions to help position itself as a leader in normative values: tackling human rights, addressing corruption on a global scale and, perhaps in time, championing environmental issues.

Until now we have seen more convergence than divergence between the UK and the EU on sanctions. The UK can now pass sanctions legislation with more speed and has greater space to diverge from European - and indeed other – allies when it feels it supports its policy goals.

Meeting sanctions challenges: globalise, then contextualise

The challenges organisations face with sanctions risk and compliance are varied and numerous, from the operational challenge of screening vast numbers of third parties to the investigative challenge of identifying individuals or entities who are currently sanctioned or could be subject to sanctions in the future.

Risk and compliance teams are increasingly looking to adjacent teams—such as public policy and government affairs teams as well as, in some cases, specialist members of ESG teams— to improve their ability to forecast and assess sanctions risk. Sanctions are a highly politicised foreign policy tool. An organisation looking to understand and future proof its exposure to sanctions, needs to look at global political developments and then contextualise those developments within the national politics and economics of specific countries.

A conversation with Justine Walker

I recently interviewed Dr. Justine Walker, Global Head of Sanctions, Compliance & Risk, ACAMS, to discuss the outlook for sanctions and key challenges The following is an excerpt from our conversation, which you can hear in full on our Legal and Compliance Insights podcast.

Henry Smith

Justine, I'd like ask you about some of your work at ACAMS helping the private sector engage with governments on their pain points and challenges with sanctions. What is it that you hear most regularly?

Justine Walker

Complexity of implementation is the headline point. Sanctions have evolved in such a phenomenally challenging way. 15-20 years ago, you were really looking at the name of an individual or entity—where were they sanctioned? You had some major regimes, whether it be around Iraq or around other regimes where there were certain prohibitions, or indeed comprehensive bans. But today we have a much broader type of targeting of individuals, entities or country programmes. The difference between what is prohibited and what is permissible is now very, very grey.

When we see a new sanctions regime come online, there are always a lot of questions. We often see foreign policy coordination to impose sanctions, but rarely on licences and FAQs. If you go back to the Russia-Crimea-Ukraine situation in 2014, the US came out very quickly with FAQs, while it was months before the EU came out with similar clarification.

So I ask, what are the most complex issues of the day? Where do we need to identify public private sector dialogue?

Over the past year, we've been doing quite a lot of work around the maritime sector and a lot of work around some of the China-focused sanctions. We've just started a project around managing sanctions risk within ransomware payments. You have these big thematic issues, which are very, very global, and there needs to be consensus in the public-private sector around permissible versus prohibitions—what is allowed and isn't allowed.

But there's also another dynamic, which is equally important, and that's the screening and due diligence side of things. A lot of scenarios where we see sanctions breaches, it's because the basics haven't been implemented appropriately, and the screening systems haven't been set up correctly. It's important to clarify: what does a good compliance program look like? And this extends beyond regulated financial institutions—who may be a bit more familiar with those types of concepts—to all players, whether they're a big corporate, small corporate or humanitarian actor. Sanctions really impact a much broader group of people.

So you have two elements of that public-private sector dialogue. One is simply: what do these regimes mean? What is permissible? What would be the risk element, legally or reputationally? How do you ring fence certain elements? But there are also the nuts and bolts, the basic elements. How have you set up your screening? How are you training your staff? How are you looking at ownership and control—because we know that ownership and control is very different in, for example, the US, the EU and the UK. Those fundamental differences can be quite critical to whether you are actually violating sanctions.

Sanctions is an exciting area, it evolves weekly, daily, sometimes hourly. But there's also underpinning elements. And that's why we balance our engagement on both aspects.

Henry Smith

I think what you really brought to life there was the combination of needing to understand the macro political forces that shape geopolitics—and thus where sanctions might go—but also the minutiae of what an organisation needs to have in place to ensure that it complies with different sanctions regimes.

It's a bit of a double-edged sword in some ways, with the level of guidance and FAQs available—particularly in the US and increasingly in the UK and the EU—about sanctions compliance. It's helpful for organisations, whether regulated financial services or broader corporates and private equity firms. They can look at this guidance; they can build systems and processes around it. But now there is an expectation for organisations to have a certain level of sophistication in how they consider and evaluate sanctions risk—how they choose to comply with different regimes.

Justine, are there any potential surprises or emerging trends with sanctions in the year ahead, perhaps topics that aren't getting the attention yet that you think they deserve?

Justine Walker

So I used to be really good at looking at the year ahead and predicting the use of sanctions and how and where they might arise. I think it's becoming much more difficult to predict.

Three years ago, we wouldn't have identified China as being so complex; we wouldn't potentially have indicated that Russia would be under the spotlight it currently is. Afghanistan is another one. So we've seen three major sanctions regimes, which, for those of us in the sanctions community, weren't quite in tune with wider geopolitical risk. For me, predicting what might happen in the year ahead, I think you absolutely need to align your sanctions planning scenarios. But also, you need to align that closely with geopolitical risk—where are the hotspots going to be in the world which may trigger sanctions?

One area that I don't think is being given the spotlight it currently deserves is supply chains. We saw in December the Uyghur Forced Labor Prevention Act passed in the US. That act could be really fundamental in changing how people assess risk around supply chains. For me, that's one that anybody in the corporate financial world should absolutely be watching.

I mentioned ransomware earlier on, and I think that we could potentially see more complex sanctions come forwards. So that's a new emerging threat. Western governments—whether it's Australia, Canada, the UK, EU, US—they're all focusing much more on cyber. And they can use sanctions as a tool to mitigate against cyber threats.

And obviously, if we have a major upscaling in sanctions between major economies, counter sanctions as we are seeing in late February 2022 against Russia, are going to be the big one moving forwards. I am advising everybody I work with to really look at how they may be impacted by counter sanctions. Do they understand their exposure to different jurisdictions? Are their contract clauses appropriately designed? Can they accept relationships if they need to without being sued? There's a lot to think about, and there's a lot of elements that we could see develop over the next 12 months.

Henry Smith

Your supply chain point, I think, is one that is very pertinent, and the sanctions considerations there are also being wrapped up in other trends that are driving greater scrutiny of supply chains, not least the broader ESG agenda and some of the additional diligence requirements that are being imposed by governments around the world.

Ransomware is clearly an area that is of interest to Control Risks clients, both in a proactive sense of understanding how it is that they might address ransomware considerations, but also in a reactive sense, when they unfortunately experience a breach of some sort and need to quickly understand what it is that they can or can't do.

We're also seeing questions from clients around how they can get ahead of these potential flashpoints. Look at the range of coups that there have been in parts of Africa over the past year, the deterioration in the situation in Myanmar, as two recent examples, and - as we discuss this - the rapidly evolving and dangerous Russian invasion of Ukraine. One of the ways that we've responded is by developing a series of sanctions risk ratings.

We build these on a jurisdiction-by-jurisdiction level and then look at different sector impacts within specific jurisdictions. We revise the ratings as and when we see political events coming, or in response to political outcomes.

I think one final area of surprise and evolution in sanctions is whether different governments will begin to look at environmental harm as a justification for sanctions action. I think that it would probably be the EU that would try to position itself as a leader here. The EU does try to use sanctions to position itself or to position its values around the world. And we know that the EU has been one of the leaders in the broader ESG agenda.

Justine, thank you so much for taking the time to talk to me today and for sharing your insights. It's been a real pleasure.

Justine Walker

Henry, it's always a pleasure to speak to you, and I've enjoyed our exchange today.

We are providing monitoring of sanctions to subscribers to our political risk and sanctions monitoring services. Find out more about Russia/Ukraine monitoring here, and learn about our Sanctions Country Monitor here.

Authors

Henry Smith
Partner
Control Risks

Justine Walker
Global Head - Sanctions, Compliance and Risk
ACAMS

The view from the US

In its review of US sanctions policy last year, the US Treasury signalled a return to the era of "smart sanctions" designed to minimise unintended impacts on business and society. It also underscored the importance of multilateral coordination with partners and allies, and using sanctions to pursue clear, specific foreign policy goals. The Treasury pledged to develop new ways to evaluate the impacts and effectiveness of sanctions.

This was not the first time a new administration had set similar goals, but the sanctions policy review was welcomed by the regulated community, still reeling from four turbulent years of the Trump administration when sanctions and related actions reached a new high in aggressiveness. However, while the first year of the Biden administration brought a change in tone to the use of sanctions, it did not reveal a change in the emphasis on sanctions: they remain a central piece in almost all major foreign policy challenges.

Moreover, even if the Biden team was to bring meaningful reform to the use of sanctions as per its review, such a change in policy approach would not reverse the legal reality of strict enforcement and steep penalties for sanctions violations. Organisations will still be expected to implement robust sanctions compliance programmes in line with guidance from the US Treasury's Office of Foreign Assets Control (OFAC). Additionally, regardless of sanctions policy, in order to effectively manage sanctions risks, organisations must also pay close attention to emerging trends and areas of geographic and thematic focus.

Emerging trends

Multilateralism

The power of US sanctions derives in part from the tool's ability to weaponize the size and role of the US financial system in the global economy. Additionally, the US Treasury and other agencies have honed their skills over the last two decades to more effectively marry this innate economic power with a nuanced use of financial intelligence, enabling the US Government to identify and designate meaningful sanctions targets. Despite their unilateral strength, coordination with allies and partners on policy and implementation has become increasingly necessary to maintain sanctions effectiveness as the targets have become larger and more economically sophisticated.

To this end, as part of its broader outreach to partners and allies, the Biden administration is actively working to coordinate sanctions, including recent actions on China, Belarus, Myanmar, Russia and Nicaragua, through the Group of 7 (G7) and other fora. Notably, in many cases the US is favouring bilateral and "mini-lateral" sanctions dialogues over action at the UN Security Council, where geopolitical competition with Russia and China increasingly stymies sanctions initiatives.

Counter-sanctions laws

Increased multilateral coordination, however, will not eliminate significant divergence in sanctions policy – even among close allies. The US blockade of Cuba is unlikely to be altered in the near term, for example. Convergence with Europe on Iran sanctions depends on fragile nuclear negotiations.

In addition, international companies face an expanding web of laws and regulations designed to deter compliance with US sanctions. The EU is in the process of updating its 1996 blocking statute to strengthen resilience to and deterrence of "unlawful" foreign sanctions. Russia continues to debate criminal penalties for compliance with "unfriendly" US and European sanctions, while China in 2021 rolled out regulations patterned on the EU blocking statute prohibiting compliance with "unjust" foreign laws and a new Law on Countering Foreign Sanctions. It remains unclear how China will enforce its blocking regulations, we have already seen Chinese companies increasingly push back against erstwhile boilerplate provisions in contracts and agreements confirming compliance with US sanctions. (*Note that US sanctions on China are limited and targeted, with modest impacts on business*.) In this regard, the direction of travel is clear: companies will increasingly need to consider how compliance with US

and international sanctions carries its own political, reputational, and legal risks – and, short of contractual provisions, how best to ensure compliance with all relevant and applicable regulations.

Digital currencies

The US Treasury report identified concerted efforts by adversaries, allies, and non-state actors to reduce exposure to the US financial system as a key challenge to sanctions efficacy. These "sanctions proofing efforts" include the establishment of non-dollar payment systems and barter relationships. The report also identified the growing use of digital currencies as an emerging sanctions risk issue – and a commensurate focus of regulatory attention and sanctions enforcement.

Accordingly, OFAC alongside the report issued guidance to digital currency companies on complying with sanctions, outlining industry-specific ways to implement its standing Framework for OFAC Compliance, such as geolocating and blocking IP addresses from sanctioned jurisdictions. OFAC since 2018 has also included digital currency addresses in Specially Designated National (SDN) listings.

These sanctions actions dovetail with a range of US regulatory efforts addressing digital currencies, including strengthened anti-money laundering (AML) requirements for cryptocurrency exchanges, signalling an increased compliance burden for digital currencies and adjacent sectors.

Issues to watch in 2022

Russia

Russia's military build-up around Ukraine, meanwhile, raises the prospect of a major expansion of US sanctions which were in the process of being expanded in late February 2022. The Biden administration has forecast that it will impose crippling and unprecedented economic and financial measures in response to a military invasion of Ukraine, including restrictions on financial transactions and sweeping technology export controls. Members of the US Congress want to go further, proposing to sever entirely Russia from the SWIFT banking network, sanction its mining sector.

The US is prepared to move quickly and unilaterally in response to an invasion but hopes to coordinate measures with European and international partners and allies. The collaboration with European governments and other allies in late February 2022 towards sanctions on Russia was striking in its pace and cohesion. Indeed, Europe has been setting the pace of US sanctions against Russia.

Iran

Halting, indirect US negotiations with Iran over its nuclear programme continue but delays progressively reduce the likelihood of a mutual return to compliance with the 2015 Joint Comprehensive Plan of Action (JCPOA). As Iran advances its nuclear programme, US negotiators see the window for diplomacy shrinking. Meanwhile, an increasingly hard-line Iranian government seeks guarantees against future sanctions that the Biden administration cannot credibly offer.

If a deal is reached in 2022, it could allow Iran to significantly increase its oil exports and conduct more international financial transactions. However, as under the JCPOA, the bulk of primary US sanctions would likely remain in place and continue to deter many international companies with US exposure from transacting with Iran.

North Korea

After a period of quiet during the Covid pandemic, North Korea since late 2021 has resumed ballistic missile tests. These so far remain below the threshold of a major provocation or global security threat, attracting only incremental US sanctions. Pyongyang's relative restraint is likely to last at least through South Korea's presidential election in March 2022. Beyond that, however, there is a persistent threat of re-escalation on the Korean peninsula, posing a renewed challenge to the US's "maximum pressure" sanctions campaign.

Human rights, corruption, and democracy

The Biden administration emphasises human rights, anti-corruption, and democracy promotion as part of its "values-based" foreign policy. It established anti-corruption as a core national security interest in mid-2021, pushed the G7 and international community to tackle forced labour, and held a virtual international democracy summit in December 2021.

US sanctions policy is in the vanguard on all three fronts. The Biden administration, like its predecessor, is making active and expansive use of Global Magnitsky thematic sanctions to target kleptocrats, human rights abusers, and autocrats worldwide. These triggers are also central to escalating sanctions regimes targeting Nicaragua, Belarus, and Myanmar. The US Congress also increasingly promotes sanctions as a response to allegations of human rights abuses.

Concurrently, the Treasury report highlights the goal of ensuring that sanctions do not impede humanitarian relief. While US sanctions typically exempt humanitarian goods, administrative hurdles and compliance risks often deter legal transactions. This has been seen clearly in the Afghanistan context where, following the US withdrawal and the return of Taliban controlled government, the sanctions status of the Taliban significantly reduced the appetite and ability of aid agencies to deliver much-needed assistance. The Biden administration has sought to provide and publicise sanctions exemptions for humanitarian relief, including related to the Covid pandemic.

Managing sanctions risks

As is clear from its first year in office, the Biden administration will continue the trend of active and expansive use of sanctions in US foreign policy. This is likely to involve more targeted implementation, more coordination with partners and allies, and more emphasis on human rights, democracy, and anti-corruption. It will not entail reduced enforcement.

Overall business risks from sanctions will remain elevated. Even if US sanctions become more coherent, international companies continue to face a complex environment marked by a proliferation of sanctions policies, lists, and triggers. Furthermore, expansive use of sanctions by the US and its allies is driving the adoption of countervailing measures, which – though currently limited – may pose compliance conflicts for some companies. In addition, sanctions are only part of a broader, overlapping compliance challenge that includes export controls, import restrictions, tariffs, and investment restrictions.

As a result, it is more important than ever that companies continue to strengthen sanctions compliance programmes in line with guidance from OFAC and undertake other good practices, including risk assessment, training and awareness, due diligence (including into supply chains), and a suitable management framework.

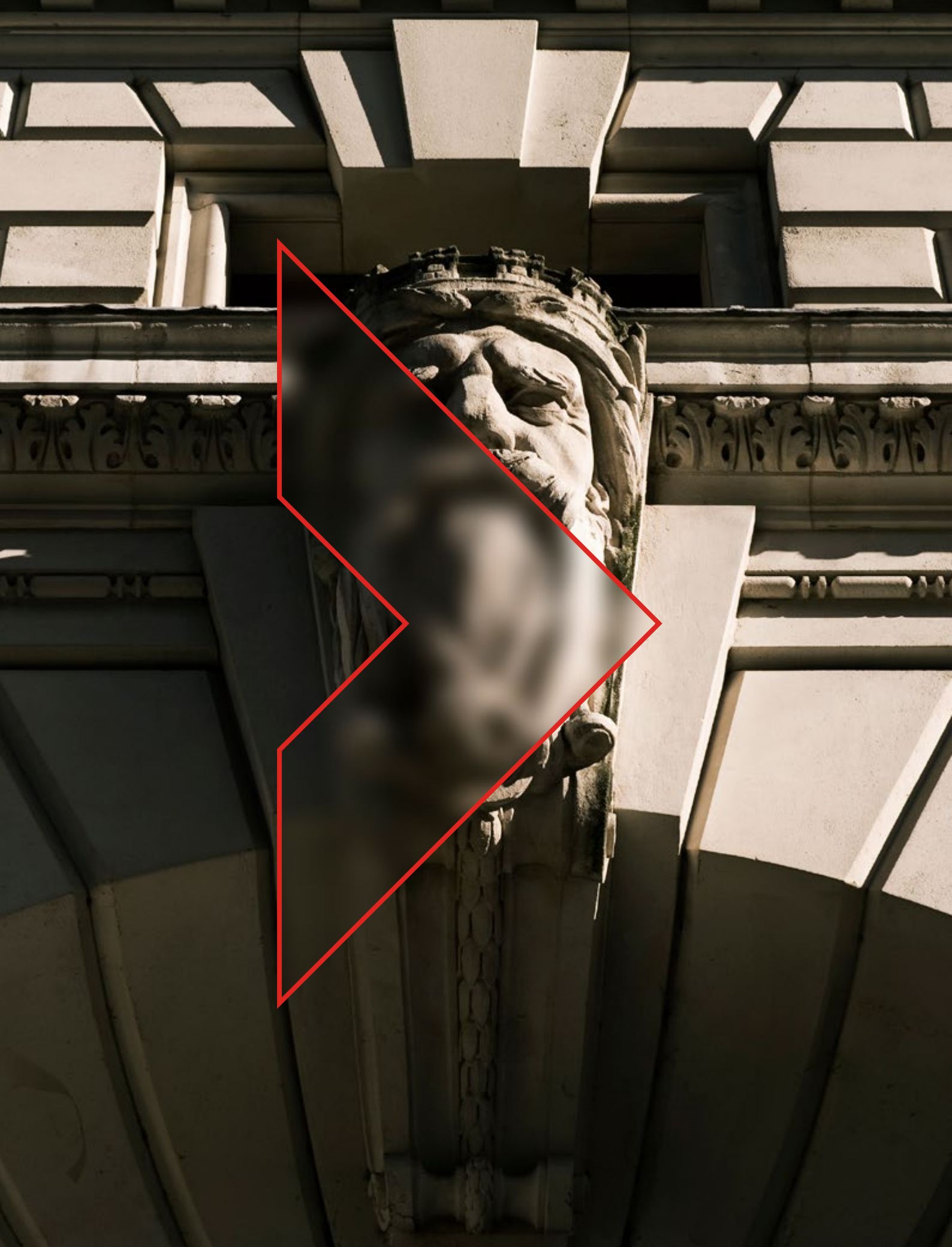
New tools and information sources can help automate and inform aspects of sanctions risk management, like benchmarking an operational footprint or supplier network. Technology is also an integral part of transaction monitoring, screening, and counterparty due diligence – especially in emerging areas like digital currencies.

Fast-moving geopolitical developments will oblige companies in 2022 to ensure that sanctions risk teams are diverse and cross-disciplinary. Legal, sales, compliance, human rights, government relations, and risk teams need to be on the same page.

Authors

Jonathan Wood
Principal
Control Risks

Adam Smith
Partner
Gibson Dunn



The view from the UK

In July 2020, the UK heralded the implementation of the UK's first post-Brexit sanctions. At the time, the UK was still in the transition period that saw it covered by most EU laws until the end of that year. The UK presented Brexit as an opportunity for an independent path for the country, with a around of sanctions on individuals and entities for human rights violations, without any publicly acknowledged coordination with the the EU and other allies. However, Russia's invasion of Ukraine in late February 2022 placed collaboration and consensus firmly on UK government's agenda with the EU.

A new start

Despite this, the trajectory of UK sanctions policy since then has not seen the country go it alone completely. The form of sanctions applied since 2020 may have diverged from that applied by Brussels, but the occasions on which the UK has applied sanctions, and the targets of these sanctions, remain closely aligned with those of Western allies, including the EU. This is unlikely to significantly change in the coming years. Despite the straining UK-EU relations over Brexit, the reality is that on most of the issues driving its current sanctions policies – Russia, human rights and corruption – the UK is broadly on the same page as the EU. Meanwhile, the imposition of the measures alongside the US, Canada and others underlines its desire to work in tandem with allies where possible. Office of Financial Sanctions (OFSI) Director Giles Thomson has acknowledged that '*sanctions are generally most effective when implemented multilaterally by as many countries as possible*' and we expect to see the UK continue to build multilateral support for its policy in this area.

Going faster

The UK has one crucial post-Brexit advantage over the EU though: the speed at which it can apply sanctions. The fact that the UK does not need to formally coordinate with 27 governments before applying sanctions allows it to act much more quickly. This means that the UK – along with others able to respond quickly (such as the US, Canada and Australia) – can get its sanctions in place. At the time of writing in late February 2022, the UK is and will continue to be part of a Western bloc in imposing tougher sanctions on Russia.

The past year has seen various examples of the UK's agility in this area, as well as its ambitions to develop sanctions policy in conjunction with a broad range of allies. This was an aspect of the UK's autonomous policy which was highlighted by Thomson in February 2021 who noted that '*the UK will continue to work on sanctions with key partners such as the US and the EU, but also with a wider range of partners as we showed last year in collaborating with Canada on the Global Human Rights sanctions regime.*' This was a reference to the development of the so-called 'Magnitsky sanctions' regime in 2020, and the UK has subsequently further cooperated with Canada in imposing sanctions under these regimes against Belarus in response to human rights violations (notably they were able to do so more quickly than the EU).

Only just getting started

The OFSI also has broader powers that it is only beginning to flex. 2021 saw the publication of the first two general licences under the Sanctions and Anti-Money Laundering Act 2018, authorising activities which would otherwise have been prohibited under sanctions regulations relating to Russia and Belarus. OFSI also issued a general license for wind down transactions with VTB in late February 2022. General licences represent a concept which the UK has borrowed from the US and give the OFSI a flexibility that does not currently exist under the EU sanctions regime.

Critical issues to watch in 2022

The UK has seen nearly five years of political drama since the vote to leave the EU in 2016, and 2022 will be no different. The government will be focused on pandemic recovery, inflationary pressures, and its own survival. However, foreign relations – and the use of sanctions to promote foreign policy objectives – will also be important. Whilst the UK government has over the past two years not considered sanctions policy to be high on its priorities list, international

developments may force it up the list. Most notably, the UK (along with its allies) has had to consider its options to respond to Russia's activities towards Ukraine, while developments in Africa, Asia and the Middle East will also be high on the agenda.

The UK government and the OFSI started 2022 with pressure to tackle two issues. First to illicit finance in the UK, in large part driven by developments in Kazakhstan and Russia. Secondly to demonstrate more enforcement activity in response to sanctions violations given the limited outcomes since the OFSI's launch in 2016. Political pressure should have limited bearing on enforcement outcomes, though an expanded scope of UK sanctions, greater resourcing to tackle economic crime, and specific investigations developing into their latter phases may encourage more enforcement actions announced in the year ahead.

Getting compliance right: key principles and guidance

As evidenced by the changing landscape of UK sanctions over the past two years, this is a dynamic and complex area which poses several risk and compliance challenges. Companies operating in the international economy should ensure that they have an approach to sanctions that meets the expectations of the UK and other relevant regulators, but is also able to implement and follow developments. This will include instituting risk-based policies and procedures to address the sanctions risks relevant to its business and third-party relationships, regular training (particularly for employees who are exposed to these risks) and buy-in and oversight from senior management.

Authors

Alexandra Kellart
Analyst
Control Risks

Katie McDougall
Partner
Norton Rose Fulbright

Cloudesley Long
Associate
Norton Rose Fulbright

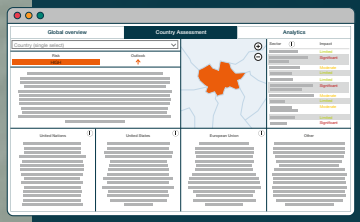
100 country risk analysts in 30 locations around the globe covering 224 territories

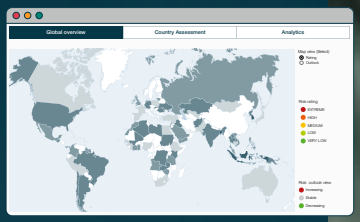
Introducing Control Risks' Sanctions Country Monitor, providing intelligence on sanctions risks globally.

Control Risks' Sanctions Country Monitor is an easy-to-use dashboard that helps organisations assess and monitor sanctions risks worldwide. Your compliance and legal, and strategy and investment teams can use our country-level sanctions risk ratings to identify sanctions exposures in new deals, projects and third-party relationships, informing your risk assessment and subsequent due diligence. The Sanctions Country Monitor can help you

- Evaluate and monitor the risk profile of countries
- Determine your risk management priorities in specific markets and sectors
- Benchmark your organisation's sanctions risk footprint
- Calibrate the required depth and frequency of your third-party screening and diligence
- Map sanctions risks to investment opportunities and supply chains
- Understand how politics and geopolitics are shaping sanctions risk

Control Risks' Sanctions Country Monitor provides the context and insight that you need to take a risk-based approach to your material sanctions exposure.





Find out more

The Sanctions Country Monitor is available through an annual subscription contract or as an add-on to existing CORE +Experts risk management platform subscriptions. For more information or to arrange a demo, please contact us at

SanctionsCountryMonitor@controlrisks.com
www.controlrisks.com/sanctionscountrymonitor

controlrisks.com

The view from the EU

The EU increasingly uses sanctions and other economic measures as a weapon of first resort in major international crises. Member states have shown their willingness to impose and absorb the economic costs associated with sanctions, and the current self-styled "geopolitical" European Commission is looking for ways to project Europe's independent geo-economic power. As such, EU sanctions are set to proliferate further and to take increasingly complex and enduring forms.

Proliferation of sanctions

The EU's Common Foreign and Security Policy (CFSP), which was agreed in 1993 and enhanced by the Treaty of Lisbon in 2007, embeds "restrictive measures" (sanctions) among the EU's foreign policy tools. Member states impose these measures on non-EU countries, legal entities, and individuals to support the EU's interests and values. All EU member states are obliged to enforce EU sanctions, and some maintain autonomous sanctions regimes as well.

Until Russia's annexation of Crimea and the launch of conflict in eastern Ukraine in 2014, the EU generally treated sanctions as a policy of the last resort and rarely imposed sanctions except as required by the UN Security Council. Since 2014, economic sanctions have become one of the most prominent and effective elements of EU foreign policy and support its ambition of achieving greater strategic autonomy.

Although the EU tends to adopt targeted sanctions against individuals and legal entities on a thematic basis, several more comprehensive and costly sanctions target entire sectors as a way of sanctioning a country's economy. After Russia, the most significant among them are sanctions targeting the current government in Belarus, its security apparatus, and its key sources of income.

Deterrence tool

The EU also increasingly uses the threat of sanctions to deter countries and individuals from policies and activities. If the European Council agrees framework sanctions, it demonstrates that there is unity and consensus amongst member states and there will be no internal differences in the EU.

The European Council in 2019 agreed a framework for restrictive measures in response to Turkey's unauthorised drilling activities in the Eastern Mediterranean. The framework made it possible to sanction individuals or entities responsible for or involved in the drilling of hydrocarbons, though only very limited restrictions were imposed. The adoption of a framework without specific designation was aimed at deterring further drilling activity and any international support for these actions.

The EU had spent many years divided on Russia given variations in member states' assessments of their exposure to Russian energy and its broader economy, and their view of the political and security threats that Russia posed. The pace and severity of Russia's invasion of Ukraine in late February 2022 changed the individual and collective calculus of member states, generating consensus about a raft of significant economic sanctions and other measures against Russia.

Energy crisis and climate agenda

The EU's initial sanctions against Russia in late February 2022 contained politically important decisions, such as Germany suspending the NordStream 2 gas pipeline, though stopped short on designating important Russian energy companies or barring the exports of Russian gas. The decision to escalate sanctions to include measures of this nature would like require and escalation in Russia's invasion of Ukraine or other measures against other Europe countries.

The EU will continue to position itself as a global leader in efforts to mitigate climate change. It operates the world's largest carbon market, is considering a carbon border adjustment mechanism (CBAM; carbon tariff) on emissions-intensive imports and could wield sanctions against major polluters in the future. The potential for thematic sanctions focused on climate related issues might emerge as a new challenge for sanctions professionals, though others are already raising concerns.

Human rights, rule of law and corruption in focus

Since the adoption of the EU Global Human Rights Sanctions Regime in December 2020, the EU has emphasised sanctions against human rights abusers. The European Council in 2021 imposed several rounds of sanctions against individuals and entities which it deemed responsible for serious human rights violations and abuses in Russia, China, North Korea, Libya, South Sudan and Eritrea.

In 2020 the Council also agreed on a framework for targeted sanctions against people and entities "responsible for undermining democracy or the rule of law in Lebanon". The framework is the "stick" in the EU's efforts to promote government accountability and anti-corruption investigations in Lebanon, albeit with limited success so far.

The European Parliament is also increasingly driving a more extensive emphasis on human rights and corruption as a basis for targeted sanctions. In 2021 the Parliament passed a resolution calling on the European Commission and member government to impose anti-corruption sanctions on Russians suspected of fraud and graft. Although no such decision was adopted by the European Council, the trend towards greater emphasis on designations related to human rights and corruption is likely to continue in 2022.

Transatlantic cooperation

Transatlantic sanctions cooperation and coordination has improved significantly since US President Joe Biden entered office. The EU and US coordinated closely on their response to Russia's invasion of Ukraine in late February 2022, and in 2021 coordinated sanctions against Myanmar and other countries. The EU undoubtedly approves of the US administration's desire to limit the impacts of US sanctions on European companies.

Nonetheless, given the potential for US policy to swing abruptly with a future change in government, the EU is also taking steps to insulate itself from US sanctions. In December 2021, for example, the EU Court of Justice (ECJ) issued a long-awaited interpretation of the EU's Blocking Statute for the first time since its adoption in 1996 (in response to the US embargo of Cuba). The ambivalent ruling upholds the Blocking Statute but potentially shields companies that comply with US sanctions to avoid "disproportionate effects" on their business. It will remain at the discretion of member states how to enforce the Blocking Statue, though private actors have used it as the legal basis for claims against entities that have not fulfilled contractual obligations through their compliance with US sanctions rather than EU sanctions.

Political consensus-building and uneven implementation

Although sanctions have become one of the most frequently used tools of EU's foreign and security policy, decision-making on and enforcement of economic restrictions have been politicised and inconsistent.

Sanctions decisions – particularly those that are reactive to crises – are taken by member-states by consensus, which often entails lengthy and messy negotiations, last-minute decisions, and fraught compromises. In September 2020, the EU failed to agree a package of sanctions on Belarus after Cyprus blocked the plan citing the lack of action against Turkey. When sanctions were imposed in October

2020, Belgium pushed for a major loophole in sanctions against Belarus's potash sector. As a result, despite several rounds of sanctions, trade with Belarus actually increased in 2021.

The decisions about sanctions against Russia in late February 2022 demonstrated a new found unity and purpose in the EU, which had been absent in previous discussions about Russia. The EU's ability to sustain this with Russia will be influenced by a variety of security and economic consequences as the conflict plays out, though the consensus at the time of writing has been striking in the pace at which it was reached in response to the invasion.

Sanctions enforcements is by individual member states

Although the European Commission is responsible for enacting EU sanctions, member states continue to oversee their implementation and enforcement. Member-states are also responsible for determining penalties for sanctions violations and granting exemptions. However, member states have varying institutional capacities to investigate and decide violations. Furthermore, governments are often reluctant to penalise domestic companies for violations that might not incur penalties elsewhere in the EU. As a result, sanctions implementation varies widely across the EU, which will continue in 2022.

In summary, EU sanctions will increase in breadth and complexity, through a mixture of jurisdiction specific, and thematic sanctions. The Biden administration has more common ground than divergence with the EU on these sanctions, though there will be inconsistency between the EU and the US, the UK, and other countries' sanctions regimes, which will make compliance more challenging from a political and regulatory perspective. And while sanctions monitoring typically focuses on foreign policy and geopolitics, organisations will also need to understand the EU's internal politics to pre-empt and manage sanctions risks.

Authors

Jonathan Wood
Principal
Control Risks

Anna Walker
Director
Control Risks

The compliance challenges of Western autonomous sanctions regimes

Given the significant compliance burden from US and EU sanctions, the challenges posed by other regimes are often overlooked. Some countries, including Russia, China, Ukraine and several Gulf states, impose limited economic and diplomatic sanctions, but generally do not use them extensively beyond specific bilateral relationships and circumstances. Autonomous sanctions partly reflect the intensification of geostrategic competition between Western powers on the one hand and Russia and China on the other.

However, a range of Western countries are following Washington's lead and increasingly relying on autonomous sanctions regimes as a tool of foreign policy. Such regimes provide them legal authority to introduce sanctions independently of other countries and beyond those required by the UN.

Geopolitical obstacles to consensus within the UN Security Council (for example, on conflicts in Syria and Ukraine) have increased the intent of Western countries to impose their own sanctions, and demonstrably respond to perceived violations of international law and global norms.

Autonomous sanctions have also become an increasingly important area of diplomatic and foreign policy engagement among Western countries. After marching in lockstep on sanctions against Iran and Russia during the mid-2010s, the US diverged sharply from its European allies with a more unilateral and coercive approach towards Iran during the administration of President Donald Trump (2017-21). US President Joe Biden has sought to restore alignment with key US allies and partners, and has carefully choreographed sanctions announcements against Russia, Myanmar, China and Belarus.

Thematic sanctions

Within autonomous sanctions, there is a trend towards extraterritorial thematic measures, particularly focusing on human rights and corruption. Since 2016, several Western governments have followed the US in implementing so-called Magnitsky sanctions (named after Sergei Magnitsky, a Russian lawyer who died in a Russian prison in 2009 after alleged mistreatment). Before an EU-wide global human rights sanctions regime entered into force in December 2020, individual EU member states including the Netherlands and Germany had also considered adopting their own national provisions.

But human rights and corruption are not the only issues of concern. Both the UK and Norway have adopted sanctions that allow them to respond to chemical weapons and cyber-attacks with asset freezes and travel bans. Australia in December 2021 amended its 2011 Autonomous Sanctions Act to establish new thematic (rather than country-based) categories under which it can impose sanctions. Canberra will now be able to impose sanctions on individuals and entities in any location globally in relation to the proliferation of weapons of mass destruction, threats to international security, human rights violations, malicious cyber activities, activities that are damaging to the rule of law and good governance, and serious breaches of international humanitarian law. It is unique in including all these jurisdictions within a single bill.

Convergence with the US and EU

Western autonomous regimes have similar scope to those of the US and EU (and the UN). There are relatively few cases of Western sanctions on countries or in response to issues that are not already covered in some way by regimes approved by Washington and Brussels (or the UN Security Council).

Nevertheless, countries clearly have different priorities for their independent regimes depending on their foreign policy goals and diplomatic relations. For example, Latvia, Lithuania and Estonia have used their respective Magnitsky provisions to

Fig.1 › The Spread of Magnitsky-style legislation

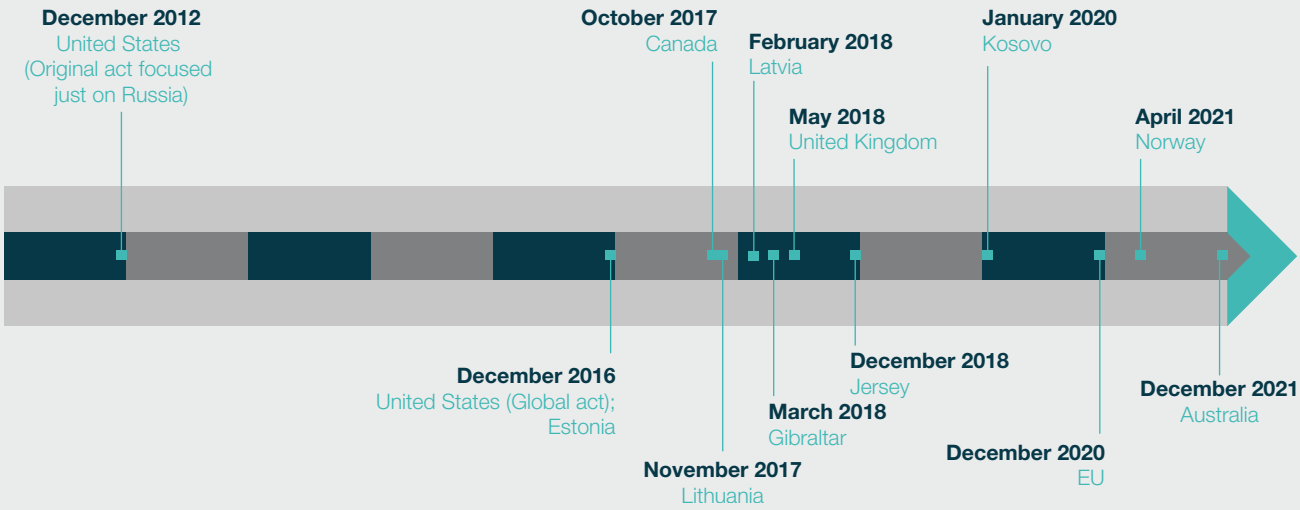
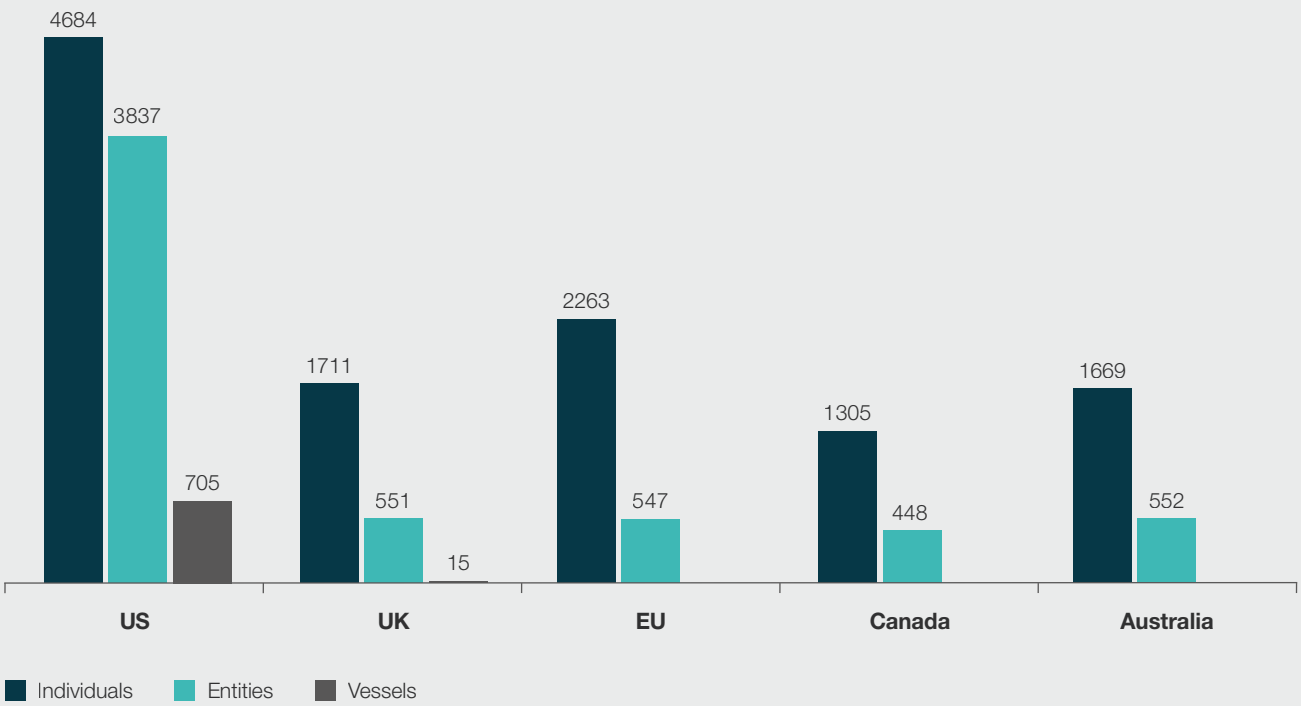


Fig.2 › Relative size of sanctions lists (as of February 2022)



Source: Consolidated sanctions lists of the UN, US, EU, UK, Canada and Australia

impose asset freezes and travel bans on Russian individuals prior to the February 2022 of invasion of Ukraine – reflecting the perennially tense relations between Moscow and its Baltic neighbours.

Many non-EU European countries align themselves with EU sanctions. Norway, for example, typically adopts decisions struck in Brussels. Other EU allies within the wider European and post-Soviet region take a more selective approach. For example, Georgia has tended to align with EU sanctions on Russia, while Armenia (which is economically and militarily heavily reliant on Russia) has not.

List divergence

As well as targeting similar countries to the US and EU, individual Western sanctions lists are often closely aligned. However, there is not complete convergence. There are many instances where third country designations differ from each other and from the lists published by the US and the EU. This can create additional compliance and legal challenges for organisations that need or want to comply with these different governments' sanctions regimes.

This is evident for some countries where sanctions risks are high and where foreign policy between the US and other Western countries has diverged in recent years. There are very significant divergences between the US sanctions on Iran and those of other Western powers. However, there are also notable differences even when the foreign policy of different Western countries does not significantly differ in other areas. Since mid-2020, the UK and Canada have imposed successive rounds of sanctions on Belarus. Despite coordinating closely with the EU and US on announcements, synchronised revelations have often belied significant divergence in specific listings. A varying appetite for strict measures reflects vastly different exposures to the Belarusian economy. A significant degree of consensus was also reached in February 2022 in the early stages of Russia's invasion of Ukraine.

Meanwhile, some countries that would otherwise seek coordination with the EU have taken measures independently, often because they can act more nimbly and more forcibly than the EU where decisions have to be made by consensus among the 27 member states.

Outlook

Autonomous sanctions regimes typically have less reach and impact than those of the US and the EU, and convergence of political interest provides some insight into the likely trajectory of sanctions risk in individual countries. However, the expanded use of sanctions and the adoption of thematic regimes by a growing number of Western countries means that companies need to consider the potential risk of sanctions exposure in a larger number of jurisdictions and broader range of possible relationships. Companies also need to think carefully about the people, currencies and legal entities that are involved in business activity so that they manage their exposure to different countries' regimes. Against this backdrop, the compliance costs of independent Western sanctions regimes is only set to grow.

Authors

Joseph Smith
Senior Analyst
Control Risks

Ransomware: where the rubber meets the road for security, compliance and legal teams

Although ransomware has existed in some form for many years, its impact, intensity and frequency have increased exponentially in the last three-to-five years. This threat is highly dynamic, with criminal groups often changing tactics, adapting targeting patterns, and ceasing and resuming operations under new guises to avoid law enforcement action. The barriers to entry are low, thanks to the commodification of the toolkits needed to carry out these attacks. The use of unregulated cryptocurrency payment channels makes ransom payments – for those who choose to pay – hard to detect. Ransomware operators exist in a sophisticated criminal ecosystem, which will continue to present operational, financial and reputational challenges to companies, as well as complex moral and ethical dilemmas.

In the US, ransomware has been designated a national security threat following repeated attacks on critical national infrastructure. The seriousness with which the problem is viewed by the US – and other national governments – is reflected in a tighter regulatory and sanctions regime and more proactive law enforcement. Paying a ransom to restore access to files and systems may seem like a short-term fix, but it rarely is and may end up violating counter-terrorism and financial crime laws locally and internationally. Companies should instead focus on enhancing their cyber security and compliance controls. Putting in place a risk-based compliance programme and sharing information with the authorities are now viewed by the US Treasury's Office of Foreign Assets Control as a "significant mitigating factor" in any post-attack enforcement action. It is the best way for a company to build resilience, but also to mitigate its exposure to increasingly costly sanctions violations.

A conversation with Jay Perera and Ed McNicholas

James Owen, Partner and global head of Cyber Security at Control Risks, recently interviewed Jay Perera, Director leading Control Risks' Cyber Consulting and Response business in Europe and Africa, and Ed McNicholas, Partner and co-leader of Ropes & Gray's data, privacy and cybersecurity practice. They discussed the evolving challenges posed by ransomware to risk and compliance teams. The following is an excerpt from their conversation, which you can hear in full on Control Risks' Legal and Compliance Insights podcast.

James Owen

How did we get to this point? Tell us a bit more about what ransomware is and how it has changed as an attack type over the last few years.

Jay Perera

This is a story that tracks the business community's growing reliance on technology. Criminals and other nefarious parties have identified this reliance on technology as a vulnerability, and that by disrupting it there may be a way to extract payment to stop the disruption.

Five or six years ago, we were responding to a lot of distributed denial of service (DDoS) attacks. Over time, organisations have moved to more complex online platforms. Attacks have evolved from trying to take down a website to targeting specific companies and their critical assets by getting into the network—usually by phishing or some other means—identifying critical data and then rendering it inaccessible and inoperable.

Threat actors used to target critical systems to take them offline and elicit a payment, but today companies have improved their data backups and resilience. Now we see the emergence of double extortion, where threat actors not only take critical systems offline, but also steal data from victims' networks. So even if the encryption fails or there is a backup ready, the perpetrator has stolen some data that they can leverage to force the victim company to negotiate or to try and make a concession. Most ransomware attacks that we have seen over the last 12-to-24 months have been double extortions.

James Owen

What about the costs of a ransomware attack–what's the break down between the extortion demand and the cost of the outage?

Jay Perera

Attacks are not just a matter of recovering systems. During a crisis scenario when technology has failed, there is reputational and legal fallout. You need to notify regulators and keep your customers reassured and updated. The costs associated with responding have increased. The regulatory environment has shifted on ransomware attacks and organisations need to act robustly.

James Owen

Ed, tell us about your experience of advising on ransomware; how has it evolved?

Ed McNicholas

These days ransomware often involves data exfiltration, or at a minimum, unauthorised access to personal data or other confidential information. Organisations must assess their obligations to issue data breach notifications, even if they pay the ransom. A few years ago, if you paid the ransom to get your system back up, the incident could be almost entirely dealt with internally. With double extortion involving data exfiltration, organisations will also face a notification decision.

These decisions are fact-intensive and time-consuming. You must look at exactly where the attacker went, how they impacted the database and assess the risk of harm to individuals. Ransomware actors often threaten to expose their target's data if they do not pay the ransom. Payment alone does not eliminate a victim's obligation to provide notification under applicable law.

James Owen

It also does not guarantee they will get their data back. There is a certain amount of crossing your fingers, isn't there?

Ed McNicholas

There certainly is. There was a study on the amount of data recovered post-ransom payment, and about 65% recovered all their data, whereas 29% apparently only recovered about half.

James Owen

And sometimes we see instances where the additional data that has been exfiltrated is ransomed a second or third time, and if a payment is made, that company is, in effect, painting a target on its back.

The US Department of Justice (DOJ) has had some significant wins lately, particularly regarding Eastern European-based groups. Do you think more pressure is being exerted on the main criminal operators, and is that likely to result in less significant attacks in the future?

Ed McNicholas

I do think offensive cyber security operations by Western countries against the sponsors of these attacks have been helpful. Law enforcement and the intelligence community have been going after some of these ransomware gangs and making inroads. The key thing is that these ransomware gangs and their infrastructure are businesses, they have costs and they want to make profits. And to the extent that we have offensive cyber operations, either through law enforcement or through cyberspace military operations, we can increase these costs.

One of the big problems with the expansion of ransomware is that it became too cheap to become a ransomware extortion organization; you had a free flow of money with unregulated crypto, a government in Russia that would allow you to operate with impunity, and ransomware-as-a-service being developed. Your operating costs were much lower, you did not have to learn everything yourself, you could in fact benefit from a help desk to get your ransomware installed, and those cost curves were pushed too low. Some of the law enforcement and military operations are increasing these costs and denying them benefits. And that will help eventually to decrease this plague of ransomware.

James Owen

Given the advice you provide to your clients in this space, how do you see ransomware shaping new rules in the regulatory and law enforcement environment in the US?

Ed McNicholas

One of the biggest movers in the US is certainly going to be the Securities and Exchange Commission (SEC). In 2021 the SEC continued to stake its claim as a leading regulator for cyber security. Five years ago, it was the Federal Trade Commission (FTC) and the state attorneys general that were the leads in US cyber security. Now the SEC is coming in, both in its role regulating financial services, including for investment advisors and broker dealers, and in its role regulating public companies.

The first time the SEC ever fined a public company over cyber security issues was Yahoo in April 2018. Since then, the SEC has issued a series of guidance documents that have pushed its jurisdictional borders. In August 2021, the SEC finalized a million-dollar settlement with British educational giant Pearson, for alleged misstatements and omissions in public filings and media

statements about a data breach. It is amazing to see the SEC using the enormously powerful cudgel of securities fraud to attack cyber security issues. But this is forcing companies to engage in much more robust disclosure of potential data security issues and in turn to look to the SEC for guidance. To its credit, the SEC is issuing helpful advice on safeguarding customer accounts, the importance of overseeing vendors and making sure your data is protected when it is outside of your systems. It has also focused on procedures to address malicious email activities. As we all know, multi-factor authentication and encryption can help decrease the exposure to all sorts of email-borne pathogens, particularly ransomware.

The SEC is also focused on managing operational risk and disclosing cyber security vulnerabilities. Having pressed a whole bunch of companies to think about whether they have appropriately disclosed exposure to vulnerabilities, the SEC is now engaged in the same effort with the Log4j issue. So we have seen the SEC push out on this issue of disclosing vulnerabilities. Chair Gensler has mentioned that the SEC is currently working on a new proposal for clear cyber security governance rules, including what he is calling "cyber hygiene", as well as incident reporting, so we will see the SEC come forward with new guidance and new regulations in 2022.

James Owen

To what extent is the SEC and DOJ action being informed by their experience of anti-corruption law enforcement and risk management as a "mitigating factor"? For example, in third party vendor management and due diligence, the Foreign Corrupt Practices Act (FCPA) has played a significant role in shaping compliance programmes. I wonder whether there are any learnings about corruption and ransomware-based cyber attacks?

Ed McNicholas

I do think that the SEC has been evolving significantly in its approach to these issues. They are seeing this now much more as a governance issue, as opposed to an issue of specific technical controls. At first, seemed focused on issues like, does the company have multi factor authentication? And do they encrypt key data sources? Now it's a question of what structures the company has in place: do they have the right people in charge of cyber security? Are there adequate resources? Is there appropriate accountability? Is there access to the board of directors and is the board of directors demanding reports about cyber security so it can exercise effective oversight by shifting from the focus on particular technical controls, and highlighting this in the boardroom? The SEC is going to be driving significant change in this area.

James Owen

Jay, do we see anything similar from a UK and European point of view?

Jay Perera

Within Europe, the work the SEC is doing is being looked at. One of the key regional priorities for Europe from a regulatory perspective is the involvement of data regulators, such as the Information Commissioner's Office (ICO) in the UK as well as the various data regulators in Europe. That is the defining feature of how companies respond in Europe now, because of the emphasis on data privacy with GDPR (General Data Protection Regulation).

Speaking from experience of dealing with the ICO, we are not just seeing notifications being issued when there is a breach but also hands-on involvement, including direct briefings to the ICO and its representatives on cases where there is deemed to be a level of impact in the public interest. That then may be used to inform relevant members of government. So, I think the regulatory bodies around data, especially in Europe, have become a focal point of good cyber incident response.

James Owen

In the regulatory space, where the US leads, others follow. This could be empowering for organisations, bringing clarity to what their compliance and governance obligations are in a breach context.

However, it is not getting any easier to identify whether there is a machine or a human protagonist at the other end of the attack. And in many cases, there are multiple layers to an attack, particularly in the context of a ransomware-as-a-service offerings, where the perpetrator is just licensing the capability from a third party. How do we know who we are dealing with?

Jay Perera

One of the key stages of any response, particularly ransomware, is attribution. Sanctions compliance requires clearly knowing the entity and carrying out due diligence on that entity prior to payment. But, in cyberspace it is much more difficult to know who you are dealing with. There are very well-known groups and the countries that we come across all the time. But these groups often operate an affiliate model, in which individual hackers essentially buy access to a ransomware tool, or a part of their affiliate networks, and carry out attacks that direct victims to their dark web sites.

When we are working with clients who are going through a cyber attack there is little gain in going through an academic review of who this group is and turning over every single stone. There are some unique identifiers but not many, and it is very easy to run false flag operations on the dark web.

You need to take a proportionate approach to understanding who you are dealing with. Forensics organisations such as Control Risks that support targeted companies help identify whether a group is who they say they are. We then look at the technical indicators of a compromise: how did they get into the network, what technology did they deploy? We look at the tactics, the

websites and communication feeds they use to communicate with the victim company and assess whether it is indeed the group we think they are. There is also no guarantee that the US Treasury won't come out and say the group you were dealing with yesterday is now a sanctioned entity. This is about risk management, especially in the US.

James Owen

Yes, there is a need to demonstrate that you have put adequate procedures in place. We know that the National Cyber Security Centre (NCSC) in the UK and the Office of Foreign Assets Control (OFAC) in the US are actively discouraging ransom payments, citing co-operation with law enforcement as a mitigating factor. OFAC is advocating for companies to ensure that they have adequate and robust sanctions compliance programmes and security controls in place. Jay, what does "adequate" look like in this respect? What should security officers and compliance leads be thinking about regarding risk management, given this new guidance?

Jay Perera

There is a huge amount of ambiguity as to what constitutes effective risk management based upon the guidance. This may be frustrating, but ultimately this ambiguity reflects the fact that not every single organisation can invest in the same way, and nor should they.

Every organisation has different requirements in terms of risk profile and controls. What any regulator or law enforcement body will want to see is that you have a well-thought through plan that is linked to the threats you have identified as most prominent—which assets might be targeted and the appropriate measures to defend them. The guidance is written to force people to think about cyber security and how they should protect their most critical assets. But in terms of how this manifests, that is very much down to each company.

James Owen

Ed, are you now seeing examples of companies in the US taking a more proactive approach to cyber risk management? And if so, who is overseeing that within the organisation?

Ed McNicholas

I'm very happy to see cyber security finally in the boardroom, and that the governance of cyber security is no longer something that is being put at the feet of IT and they are just being told to handle it. It is not sitting in the Compliance Office as a minor compliance matter. The attorneys aren't saying, well, this is our responsibility.

Now, people are looking at it and saying, wait, there is an IT aspect but, if our systems go down, this will have operational impacts and legal impacts. Preparations have compliance impacts, and the whole company needs to respond. And the way to make sure that a whole company is responding to the threat of ransomware is to have leadership from the top.

One of the most effective things any board of directors could do is to simply ask for a quarterly report on cyber security readiness. The mere need to write something down and present it to the board of directors will cause each person in the organization to think, well, I have a role in this. So, the compliance officer will submit a report, legal will submit a report and IT will submit a report. Then the chief financial officer will have to say, well, yes, I have put adequate budget towards the different operating segments of the company, and we will have to think, what if this manufacturing plant went down? How would we respond if this plant were down for a week or two? If you have that kind of thoughtful response in advance, your ability to weather any cyber- attack increases dramatically.

James Owen

Looking forward, how do we see the ransomware threat evolving? How are the regulations going to keep up?

Jay Perera

It will get more complex. I regularly talk to security teams from major financial institutions and the key thing they always mention is the simplicity of some of the attacks they are seeing. Attackers are not always taking the most technologically advanced way into a business; it is about understanding how an asset management or manufacturing firm works, for example. That knowledge and understanding helps attackers take a more targeted approach.

Regulation and sanctions compliance reduce the options for these criminal groups. If a group is known as a sanctioned entity, it will not be paid by the organisations it targets. That is effective in slowing things down and making it much more difficult for attackers. As Ed said earlier, it was becoming too easy. As we start to see these changes come through and scrutiny increases, we should start to see better law enforcement interaction and intelligence sharing, which will lead to some of the larger groups being targeted at their core and taken offline.

James Owen

Cyber insurance has contributed to the problem, making it economically viable to pay the ransom in many cases. What is your view on how that will develop, with insurers keen to counter rising claims and exposure?

Ed McNicholas

Insurance is certainly a key factor. Ransomware itself has been around for more than a decade, it had this incredible expansion, because of a series of factors that allowed it to grow from being a minor annoyance to a national security issue. And one of the concerns is the availability of insurance to pay for the ransoms.

Obviously, insurance companies do not want to foster ransomware. During this most recent renewal cycle, we have seen insurers significantly decrease the amount of coverage available while significantly increasing the cost, as well as taking a much stricter approach to underwriting

criteria. For companies, this has significantly diminished the availability of coverage for ransomware. It brings up an important question about whether an organisation should or should not pay the ransom.

Normally, organizations have had the reliability of insurance cover to support that decision, and with the guidance from the insurance companies about when to negotiate, it was enough that paying the ransom was economical. Now, a lot of companies will be approaching that decision about whether to pay, whether to negotiate then pay, or whether not to pay at all, through a much through a different framework. We are seeing governments discourage payment of ransom as well as suggest that you need to do extensive checking for OFAC and sanctions regimes before making payments.

The payment question becomes a buy versus build analysis. Can they rebuild their system, or do they have to buy back their old system? And many companies are now saying, no, we can simply build a new or better system, as opposed to paying the ransom. The issue then will be whether insurance will cover the cost of the rebuilding process, or will they say, no, that was part of your underlying IT infrastructure.

James Owen

To finish, if there was one key recommendation you would like to make to a compliance officer or security lead, what would that be?

Jay Perera

Understand some of the specific risks and look at your data. With appropriate controls, you can hopefully stop these attacks from happening. But, if you are attacked, you will be in a good place to respond. If you know your data and understand what is on your network, then if the worst does happen, you'll understand what is there. By speaking to your teams and to external counsel like Ed, you can make decisions much faster while being aware of what you need to do to remain compliant.

Ed McNicholas

My main recommendation is to get on the other side of the table, yourself in the shoes of the person who wants to attack your organisation. Although you might experience that person through a bot that they have sent out, there is a person behind it, someone who has costs and is trying to maximize profits. Think about what you can do to increase their cost curves. How can you make yourself a harder target? Think about what you can do to increase their cost curves. How can you make yourself a harder target? And if you analyze it that way, you are going to be focused on inflicting the maximum costs on your adversary, and it becomes a thought experiment that can be very useful in deciding whether you should put more money into insurance, multi-factor authentication, training your employees to spot phishing, or conducting a training session or tabletop exercises for your board of directors. If you think about the relative rate of return of these various potential investments, you will have a better overall strategy.

James Owen

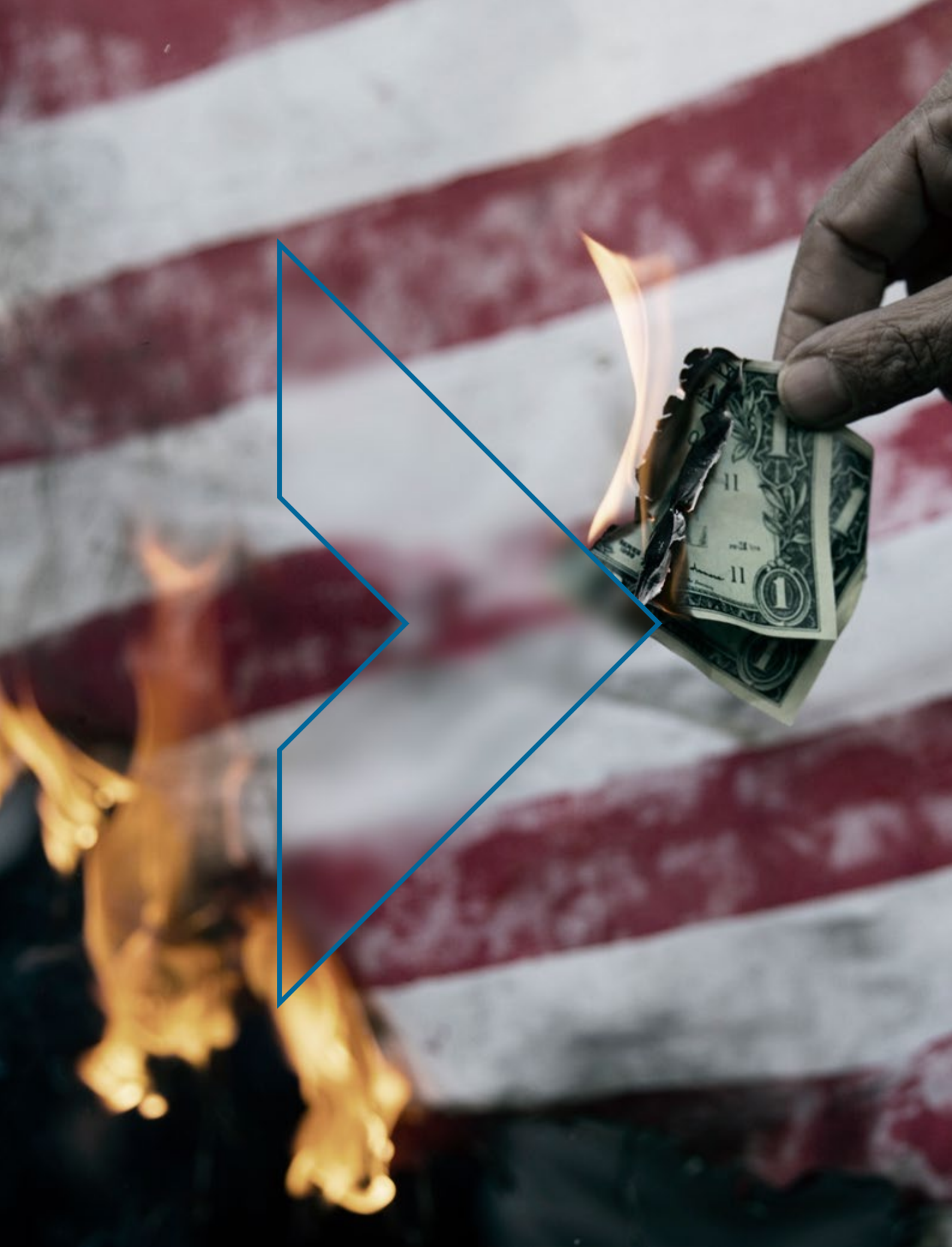
Many thanks to you both for those valuable contributions.

Authors

James Owen
Partner
Control Risks

Jay Perera
Director
Control Risks

Ed McNichols
Partner
Ropes & Gray



Sanctions considerations in cross-border transactions

Assessing exposure to sanctions and broader financial crime risks is a critical diligence consideration when thinking of investing in any cross-border transactions. The continued expansion and increased complexity of sanctions regimes, greater frequency of regulatory changes, and escalating enforcement has made this more important and more challenging to assess during the diligence process in recent years.

Here we use a fictional case study to outline the steps that buyers can take to identify, evaluate, and address sanctions risks, and the commercial considerations that sanctions compliance can cause. Though not intended as an exhaustive diligence and risk assessment, it raises the process and considerations for buyers. We note that this article was written in February 2022 and some of the analysis of the sanctions against Russia is likely to have changed since publication.

Introducing our case study

This case study assumes a US and a European fund are co-investing, with the US entity taking the majority position. Their target is a business unit carved out of an industrial company headquartered in Germany. The target is reliant on agents and distributors for business development and revenue, some of which sell its products in Cuba and Iran. Finally, it has a manufacturing joint venture with a company that is owned by a Russian oligarch, with onward sales to Russian clients. Turkey is its third largest sales market after the US and EU.

Our pre-transaction diligence consists of an inside-out legal assessment and an outside-in investigation. The findings of each of these workstreams inform the other. We then outline post-transaction considerations. However, it is worth stating that from the outset of the deal it is helpful for investors and their anticipated financing parties to align on their approach to sanctions diligence, perceived key sanctions risk factors, and agree what is acceptable from a sanctions risk perspective to secure financing. This means diligence and analysis is focused on the correct issues and set within a clear framework.

Pre-transaction considerations: inside-out

There are four key considerations for the inside-out legal assessment.

- Has the Target identified sanctions as a risk area? If so, a productive first step of diligence is to understand the target's own conclusions regarding sanctions exposure (to be pressure tested as part of the diligence process), and the compliance program implemented by the Target to mitigate that risk. We consider the target's policies, procedures and supporting systems, such as screening software; the target's compliance resources and governance structure for managing sanctions risks; and whether it has monitoring and audit programmes. We would also review whether the sanctions programme is applied to the target's joint venture in Russia, particularly considering regulations that prohibit Russian parties from complying with foreign sanctions regimes.
- What is the Target's exposure to primary sanctions liability? In this case, the Target is directly subject to both the EU sanctions regime, and certain components of the US sanctions regime. Given we are considering a German company, we would look to assess which aspects of its business have historically been subject to US jurisdiction. The principal questions are whether transactions have been conducted in US dollars; involved US financial institutions, involved US persons or subsidiaries, and the use of US-origin content. We would also consider changes to primary sanctions jurisdiction because of a majority investment by a US sponsor. The US sanctions regimes involving Cuba, Iran and Russia extend directly to foreign entities owned or controlled by US Persons. Therefore, we would consider if any direct or indirect dealings with Cuba, Iran and Russia are commercially material. Any such business would almost certainly need to be wound down pre-closure unless there are general or specific licenses from OFAC

(Office of Foreign Assets Control) that could enable operations to continue under new US majority ownership. We would work with the buyer to evaluate collateral consequences of terminating business with Cuba and Iran. This could jeopardise the target's global contracts with clients or distributors and create further revenue loss than the revenue generated in Cuba and Iran. If the decision is taken to wind down the Iran or Cuba business pre-close then we look at ongoing sales contracts, ongoing service contracts, warranty obligations, the accounts receivable, and whether that is also commercially material. We would lastly consider what provisions are needed in the transactional documents to ensure such steps were completed in compliance with law and prior to closing.

- What is the Target's exposure to US secondary sanctions? The third consideration is US secondary sanctions, which can apply to business activity without a US link. We identify where direct or indirect business and entities are subject to secondary sanctions programs administered by OFAC, and whether those exposure points have been considered by the Target's evaluation. Knowing who the company is doing business with, the type of products they are selling, and the type of industries that they are supporting, we then seek to collect the relevant information to bottom out that analysis ourselves.
- Has the Target violated applicable sanctions in the past? The fourth and final consideration for the inside-out diligence is whether there have been historic sanctions violations, and if so, how they were approached and addressed, whether they were self-disclosed or been the subject of enforcement or government inquiries. As appropriate, we would assess the potential maximum civil or criminal penalties along with likely outcomes based on similar cases and experience.

Pre-transaction considerations: outside-in

We now consider the pre-transaction outside-in investigative diligence. Its objectives are to provide additional insight and context to any concerns raised in the inside-out legal assessment; identify any sanctions or additional risk considerations that are not revealed in self-declared information and management interviews with the target; and to gauge the target's culture and approach towards sanctions and broader risk management. Taken together, this gives the buyer greater confidence about the target's profile and tests their knowledge and assumptions about the deal.

- The first step is to independently review the target's ownership, control and joint ventures to ensure they are not owned or controlled by sanctioned entities or individuals. In this case, given the target's domicile and profile is in Germany it would be unlikely. The Russian joint venture partner would be a primary focus. We use the range of investigative diligence methods to do this, namely local language searches, reviews of corporate registry databases and other legal archives, and interviews with people who know the joint venture partner and its owner. These could be people at competitors, in industry bodies, from government and diplomacy, and other related fields. We would use these methods to understand the profile and relationships of the joint venture partner, and the extent to which they are sanctioned now or have a profile that means they are likely to be sanctioned in the future if additional sanctions are imposed on Russia. Beyond the partner, we would also seek to evaluate the sanctions and risk profile of the joint venture's client base in Russia to see if these third parties expose the buyers to risk. To do this, we identify external information available about the target's clients, including from government procurement databases, and then compare this with any self-declared information provided by the target. We would also use these investigative methods to see if the target's operations or sales practices touch on Crimea or separatist regions in eastern Ukraine, given they are subject to different and more extensive US, EU, and third-country sanctions regimes.
- Second step would be to look at Cuba and Iran, which are markets the target services through third parties. We would be seeking to establish the extent to which the sales are recent, and whether there is an ongoing in-market presence or sales activity. We would apply similar research techniques to those described in Russia, though also look for archived or dormant corporate entities related to the target and speak to sources with knowledge of the target's sales and distribution relationships in the country. Caution is required when considering this type of work in sanctioned countries, particularly on behalf of US clients to avoid impermissible dealings or export of services. We would work through this quite carefully to ensure everyone is comfortable with the legal parameters of the research.
- Looking beyond Iran, Cuba, and Russia, a third step is considering other countries that pose indirect sanctions exposure through diversion or third party risk (i.e., distributor, agent). The target has sales operations in markets that are not subject to significant sanctions, though are adjacent to sanctioned countries. Turkey has established trade relationships with Iran, Iraq, and Syria. We would establish if the significant sales volumes in Turkey were due to onward sales to those sanctioned markets through Turkey-based distributors or clients and if there are any red flags suggesting diversion. If we do not have access to detailed internal data, then we would be reliant on identifying external sources with a vantage point over the target's business model and third parties in Turkey. Sanctions risks, as with many financial crime risks, often appear and can be due to third party relationships, which can be assessed throughout the transaction diligence.

- As a final consideration, we would also evaluate the target's corporate culture by engaging people with a view of how the company is run, such as former employees, people at competitors, representatives of industry bodies and lobby groups, and people who hold supply or client relationships with the target. We want to evaluate how decisions are made and the extent to which the culture is inclusive and receptive to employees ranging challenging compliance related issues. This can provide helpful insights into specific issues and broader culture to inform management interviews.

Post-transaction: drawing conclusions, closing information gaps and remediation steps

Our findings from the pre-transaction diligence and legal analysis inform recommendations for the buyers to consider once the deal is closed. These recommendations are specific to the terms of the deal, the buyers' risk appetite, and the conclusions of our analysis. We raise a few hypothetical conclusions and next steps relevant to the analysis of this deal to provide a sense of the conclusions and advice that might be reached. Given the buyers would be in a controlling position post-closing, they have a helpful advantage of being able to drive improvements on specific risk areas.

We would be comfortable that the target has a good sanctions compliance program, consisting of a well-considered sanctions policy and strong supporting procedures, including a sanctions screening tool integrated into its ERP (Emergency Response Plan) system. In many cases, however, when analysing non-US headquartered companies, we find that sanctions risk assessments have been historically deficient in assessing US secondary sanctions risks. In this case we would consider additional risk assessment post-closing.

Additionally, we found that the target's third-party due diligence processes did not extend beyond screening, giving it limited oversight of its agents and distributors' sales practices and in some cases clients. This was compounded by weak contractual protections in agreements with distributors and agents and purchase orders with clients, increasing risk of indirect sanctions violations. The risk was mitigated given the lack of a historical US nexus to most of these sales as they were outside the US with non-US persons using currencies other than the US dollar, though we would note the need to monitor and assess the implications of the rapidly evolving restrictions from multiple governments on Russia. This shortcoming could be rectified post-closing by the target improving the risk assessment and diligence of third parties at onboarding; and how third parties are then monitored and audited. This would be applied to the broader third-party population rather than solely third parties in sanctioned countries or countries that trade with sanctioned countries (such as Turkey).

Looking at specific countries, we found that the good sanctions policy and processes at the corporate level were not well applied to the Russian joint venture. As such, it would be helpful to conduct a post-closing detailed forensic review of the Russia business as the target had limited oversight of its complicated network of distributors and ultimate clients in Russia. This would involve reviewing financial data on specific distributors to try and show their sales history and ultimate clients; reviewing agreements and contracts; and interviewing employees of the target and perhaps some of the third parties to understand how these distributors interact with the target and where improvements can be made. This exercise may need to be repeated and refreshed as the sanctions regimes against Russia expanded in late February 2022, and indeed a broader legal and commercial decision about whether business in Russia could continue.

We would be comfortable that the Iran and Cuba business could be wound down easily without outstanding contractual or commercial obligations, and that that would not pose a material business risk, either as standalone business or to global relationships and contracts. The practices in Turkey were indicative of onward sales to Iraq, though not Syria and Iran, though a similar forensic exercise to Russia could be undertaken to understand the extent of any sales in any of those countries. We would use similar methods to Russia, though in this case also addresses and contact information in CRM data and invoices that indicate that the end client might not be in Turkey as the target was led to understand.

Authors

Henry Smith
Partner
Control Risks

Sean Seelinger
Partner
Ropes & Gray


SIMPLEX
1-800-361-1486

Sanctions and Cryptocurrency: A challenging industry for compliance programs

On 1 October 2021, newcomers to cryptocurrency were flooded with marketing promotions to invest in Squid, a cryptocurrency inspired by a popular television show. It continued to soar throughout the month. The morning after Halloween, Squid investors learned their crypto treat was nothing more than a trick. Squid's value collapsed as its creators and developers executed an infamous "rug pull", when a coin's creators cash out their holdings of the coin, usually a significantly high percentage. Investors left holding Squid saw the value drop an astronomical 2,860%[1].

Crypto is inherently risky as an investment. Moreover, it does not take a savvy scammer to know that funds can be moved and protected from law enforcement seizures. Crucially for compliance programs, it also remains a highly effective means for sanctioned parties to continue commercial transactions anonymously. The US government has taken measures to address this new avenue to skirt sanctions regimes. Stricter regulation is certainly expected as cryptocurrency adoption increases. There are ways compliance programs can prepare and protect their organizations from accidentally transacting with a sanctioned party.

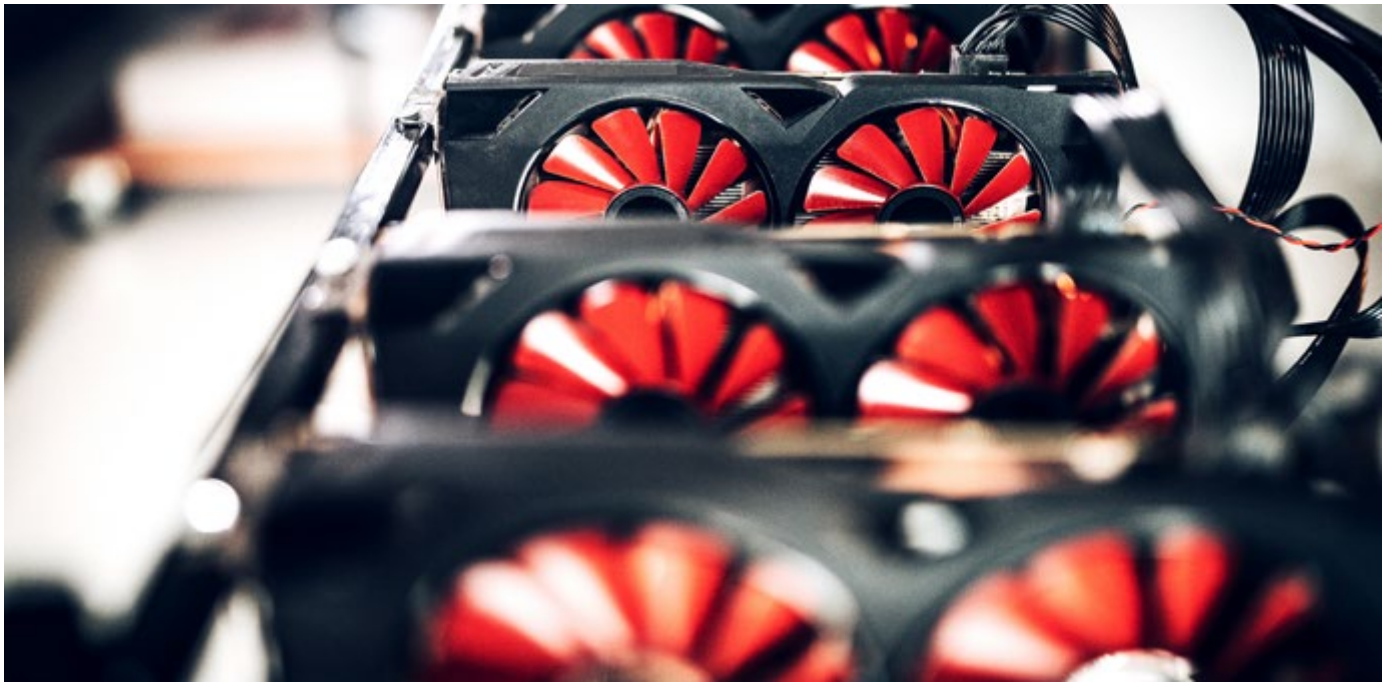
Out with SWIFT, in with DEXs

For decades, nations and individuals targeted by US sanctions have searched for ways to move their money outside the US-dominated financial system. To monitor all kinds of international payments, many countries including the US rely on the SWIFT messaging service that banks use to communicate payment instructions to each other, and on the correspondent banking system, which routes almost all payments through New York (for US transactions). It is this system, and the oversight it enables, that makes the US ability to implement sanctions particularly effective.

Cryptocurrencies offer an entirely new financial infrastructure, cutting out banks and enabling peer-to-peer transfers that bypass borders as well as regulators' jurisdictions. Cryptocurrency "mining" involves a highly complex process of verifying other users' transactions, which requires specialized hardware with significant processing power. Once mined, cryptocurrencies can be exchanged for other assets—whether hard or soft currency, or other cryptocurrencies—or traded by users directly, a process that is now simplified and facilitated by companies like Coinbase that host currencies in app-based "wallets." Instead of recording transactions in a bank's ledger, they are catalogued in "blocks" on a blockchain – a transparent, distributed ledger technology that stores data on thousands of servers at once and enables any user to see everyone else's records in near real-time.

Independent cryptocurrencies, like Bitcoin and Ether, were created with the aim of freeing money from government influence and oversight. But in recent years, states around the world have been researching to see how they can take advantage of the efficiency of blockchain technology without losing control of currency. Though no other country is known to carry out brazen crypto heists like North Korea, other states are coming to view blockchain technology as part of a longer-term strategy aimed at undermining US financial power, either by investing in the technology or by developing their own state-backed, "sovereign" cryptocurrencies, also known as central bank digital currencies.

[1] https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/



In 2018, Iran reportedly acknowledged cryptocurrency mining as a legitimate industry (although in 2021, it temporarily banned mining to conserve power supply). In December 2019, Iran's President reportedly proposed to create a Muslim cryptocurrency to cut reliance on the US Dollar. This is also a method to dodge sanctions by the US. North Korea also announced their intention to issue a digital currency, which experts believe aims to help the country bypass sanctions. Lastly, the US government acted in 2018 to prohibit transactions involving Venezuela's state virtual currency, the "Petro."

These differ from Ether or Bitcoin because they are centralized, meaning that payments can be frozen, canceled or otherwise regulated by a central authority, like a country's central bank. Many central bank digital currencies use blockchain technology, or technology inspired by it. As the manager of one cryptocurrency services provider based in Switzerland stated, "In case anyone has forgotten: The end goal of cryptocurrencies was to decentralize power, not to bolster existing centers of authority."

As with any new market, the risk evolves with new services and players. In cryptocurrency, privacy coins, digital wallets, and coin swap services all pose challenges to regulatory enforcement. However, none of these are as concerning for compliance programs as decentralized exchanges (DEX). DEXs are currently unregulated and, most concerning, do not collect standard Know Your Customer (KYC) information thus creating an ideal scenario for sanctioned parties to remain anonymous in transactions. The risk that a sanctioned person in a jurisdiction subject to sanctions is involved in a virtual currency financial exchange brings greater exposure to individuals and companies alike.

Get ahead of your risks

Companies and individuals are subject to the same sanctions compliance obligations in transactions involving virtual currencies as those involving traditional currencies. Those involved in DEX and virtual currencies are obligated and responsible for ensuring that they are not violating OFAC sanctions such as dealings with blocked persons or entities.

In November 2018, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) added two bitcoin addresses controlled by Iranian cryptocurrency brokers who moved funds from a ransomware campaign.[2] OFAC has since listed cryptocurrency addresses for cyber criminals, fentanyl traffickers, money launderers, and individuals who engaged in elections interference.[3,4,5] This is not news for cryptocurrency exchanges and digital wallet platforms, some of which have already been targeted by

[2] https://home.treasury.gov/news/press-releases/sm556
[3] https://home.treasury.gov/news/press-releases/sm756
[4] https://home.treasury.gov/news/press-releases/jy0126
[5] https://home.treasury.gov/news/press-releases/jy0471

the US government and entered into settlement agreements with OFAC for sanctions violations.

Compliance programs at companies looking to accept digital currencies may believe they are about to encounter a growing blind spot. However, they are better equipped to address sanctions risk from cryptocurrency than they may realize. There are key steps they can take, including but not limited to:

- Reviewing IP addresses and related identifying information such as a phone number or email address that may provide insight into the origination of a digital transaction. Compliance officers may simply need to speak to Accounts Payable departments to ensure this information is collected, or break through silos to facilitate the flow of this data to enterprise risk tools. Does the information show that transaction originates from a sanctioned country?
- Searching sites, such as Etherscan, that provide detailed information about blockchains including information on its value over time, transactions, and the developers.
- Identifying whether the other party in a transaction sends funds from a miner in a sanctioned country or from a country where KYC information is typically not collected. Thus, the origination of funds cannot be easily verified.

Companies should be mindful that some individuals, governments, or groups may use cryptocurrency (or virtual currency) to evade economic sanctions laws designed to isolate them. The US government expects a commitment from entities that deal in cryptocurrency to ensure that sanctions laws are complied with, and that institutions detect the involvement of designated persons or prohibited jurisdictions in transactions. In fact, departments can pull upon their experience managing antibribery risk and expectation of government regulators to hold corporations to account for the actions of their third parties, sales agents, and distributors.

Because strict liability standards apply to unauthorized dealings with sanctioned parties and jurisdictions, US persons dealing in cryptocurrency cannot avoid potential liability simply because they do not know the identity of the person with whom they are interacting. And the risk of dealing with sanctioned persons and jurisdictions when conducting virtual currency transactions will likely increase should nations like Iran and Russia further embrace cryptocurrency to try to avoid sanctions.

Three steps that help manage sanctions exposure

To protect against potential sanctions violations, there are key steps that cryptocurrency users and exchanges can take.

1. Anyone receiving or exchanging cryptocurrencies should adopt and implement KYC procedures, including sanctions screening, to identify parties trading behind the cryptocurrencies, and can employ geo-IP blocking to prohibit access by parties from sanctioned jurisdictions.
2. They should perform transaction monitoring to detect suspicious activity and file the required reports with FinCEN (US Financial Crimes Enforcement Network).
3. US persons trading in cryptocurrency should use exchanges committed to complying with US sanctions requirements. If the exchange allows sanctioned parties to participate, a US person could end up unknowingly trading with such a party and thus violating US law. Exchanges operating outside the United States that want to attract US users should also consider implementing such measures, to exclude targets of US sanctions from trading. Non-US exchanges that permit access to certain US sanctions targets may risk the imposition of US "secondary sanctions" designed to deter non-US persons from engaging in business with targets of US sanctions.

As cryptocurrency is more widely adopted, compliance departments will undoubtedly need to understand how to address risks, particularly sanctions compliance, when dealing with this form of non-traditional payment. More than in most industries, government regulators are gearing up to implement new rules and regulations. Enforcement will follow. It is important that compliance departments plan to understand how to address risks posed by cryptocurrencies.

Authors

Jeff Dexter
Director
Control Risks

Sonia Zeledón
Associate General Counsel
Ethics, Compliance and Data Privacy
The Hershey Company

Managing the challenges of sanctions screening in your third-party risk programme

International sanctions affect companies in any industry, and – as recent enforcement action has shown – companies of varying sizes. As such, sanctions are one of the most important risk factors to consider in any compliance programme. No-one wants to be found to have business ties to a sanctioned entity given the potential for significant financial penalties and reputational damage. As a result, sanctions screening has for a long time been the bedrock of any compliance programme that has to consider large numbers of third parties.

How does sanctions screening fit into a risk-based approach

We work with many types and sizes of companies with varying global footprints. One question that comes up time and again is whether an organisation needs to check all the third parties it is working with (or planning to work with) against sanctions lists or whether the application of sanctions screening could, or should, be determined based on risk. Many of our clients choose to run simple sanctions screening against all their third parties as a bare minimum. It is simply not worth running the risk of going into any relationship blind and accidentally breaching sanctions. And with about a hundred anti-terrorism or other economic sanctions lists around the world with varying degrees of significance and application it is an impossible task to check them without the help of a specialised screening solution.

The dangers of indirect or hidden links

Another challenge to be aware of with sanctions is indirect or hidden sanctions risk. The US, EU and UK dictate that companies which are 50% or more owned by one or more sanctioned entity or person are considered sanctioned themselves but they do not provide separate comprehensive lists of these entities, leaving the onus on you to find out[1].

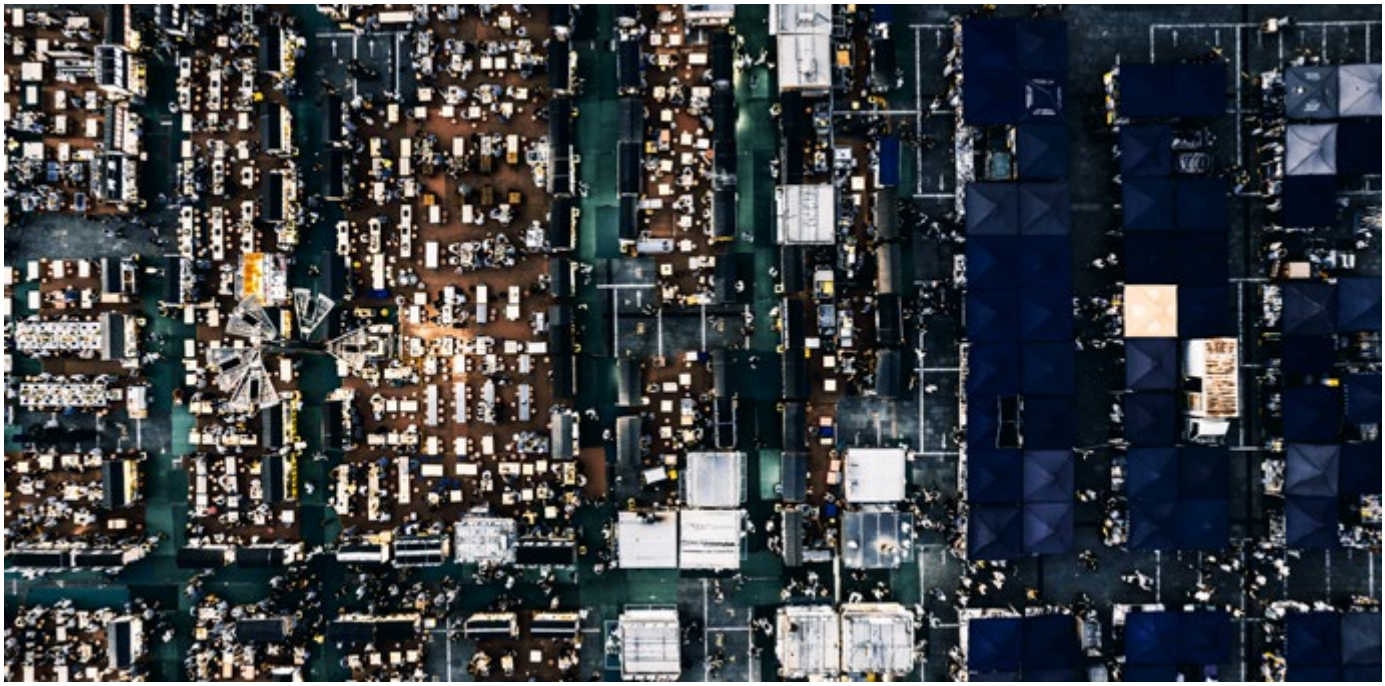
Why screening, alone, is not sufficient

Third parties can also have surprising connections that pose a sanctions risk. An entity registered in the UAE can still have links to sanctioned entities in Iran, for example. In 2018 US-based electronic manufacturer Epsilon Electronics Inc agreed to pay $1.5m to settle an OFAC (Office of Foreign Assets Control) enquiry into business transactions made with a Dubai-based distributor that then sold the goods in Iran[2]. While OFAC's investigation could not find direct proof of Epsilon's products being shipped to and distributed in Iran it found enough indication on the Dubai distributor's website of links to Iran and goods being distributed there via an affiliate, to show intent to redistribute to Iran[3]. As a result, not having sufficient information on affiliations or a good understanding of a third-party's footprint and operations could expose you to inadvertent sanctions breaches. This kind of indirect link would not be captured through sanctions screening alone, so for your higher risk third-party relationships more enhanced due diligence is needed.

[1] https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1521. In addition, the Iranian Financial Sanctions Regulations (IFSR) published by the US Treasury include affiliates and subsidiaries within their definition of foreign financial institutions. Agents and affiliates of Iran's Islamic Revolutionary Guard Corps (IRGC) are covered in various Iranian sanctions of the US Treasury such as CISADA (Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010). https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions

[2] https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20140725

[3] https://blog.volkovlaw.com/2018/09/ofac-enforcement-the-epsilon-case-and-third-party-risks/



Human-led due diligence which involves researching public records and the media, and sometimes discreet reference checks with people with a perspective on the diligence target, is an important consideration for your higher risk third parties for other reasons. Alongside sanctions, screening databases are products focused on Anti-Money Laundering and Counter Terrorist Financing (AML/CTF) specifically, and the media results they contain have this primary focus. Furthermore, to be included in the database, a media reference must meet very precise parameters - for example wrongdoing has been proven or enforcement action has been taken - within a particular set of categories and subcategories delineated by the provider. It is therefore important not to confuse the media-based searches in any of these sanctions database providers with broader anti-bribery and -corruption compliance-driven, reputational, or ESG due diligence. If you are considering a relationship from a reputational perspective or need to capture sector-specific concerns or any other indicators of potential wrong-doing, you will need to conduct human-led due diligence research.

Sanctions lists are constantly changing

Sanctions lists are not static. People and companies can be added or removed from them at any time. Without continuous monitoring of those lists, one of your third parties or their affiliates could be added to a list, putting you in immediate danger of sanctions breaches, even if you checked them before signing your contract. If you have a large third-party population, it is simply not feasible to check the lists regularly and cross-reference against your third parties, nor is it time- or cost-effective to rescreen all your third parties as frequently as needed.

Adjudicating false positive results

The idea of relevant hits brings us on to another major challenge for compliance teams: false positive analysis. How can you reliably determine whether a sanctions, or any other hit returned in a screening tool, relates to your third party and not another with a similar name? This can be an incredibly time-consuming exercise and is one of the major pain points of many of our clients. Some screening solutions, such as ours, use leading matching technology to draw on additional identifiers such as country, address, and registration number for companies or date of birth for individuals. This allows the search to provide more accurate results and reduce the false positive noise. Our solution also provides a match score based on these criteria, which can help you quickly identify those hits most likely to relate to the entity or person you are interested in.

This is not always enough to make a definitive assessment and additional research needs to be conducted to raise your confidence. You first want to look for any indication that it is not a positive match; consider the country context and whether this is a very common name; look at any unique identifying information, such as date of birth or residential address, in the screening result; and see if that could rule out the hit. After that, some general online research can typically gather enough information to determine whether a hit is likely to relate to your company or individual of interest. For a company, a website is a good place to start with online research, using information such as office locations (bearing in mind this could have moved since you were given an address), the business activity

it describes, and the names of key personnel that may be mentioned in the hit. For an individual, you might be able to find a photo that you could match against the screening information. Other times, and particularly in high-risk scenarios, you may need to go back to your main point of contact at the third party itself to ask for identifying information you have not been able to find through your own research to definitively rule out a hit.

Depending on the profile of jurisdictions and sectors you operate in, and the kinds of third parties you need to engage, you may find you get a higher or lower amount of potential hits when you conduct screening. For some of our clients, this is a straightforward task they can comfortably manage in house, for others this task is simply not manageable with a small and overstretched compliance team with limited foreign-language capabilities.

Sanctions screening is the bear minimum check for third parties, though any compliance programme will benefit from a risk-based approach, whether this is running screening with different configurations for different risk levels or knowing when to escalate to a deeper level of due diligence. However, you choose to run your screening programme, make sure you think about how you will manage the challenges of hidden risk through sanctioned affiliates; stay up to date with any changes to sanctions designations; and conduct false positive and negative reviews to make sure you are focused on what is relevant.

Author

Emily Morgan
Global Director
Control Risks