EU Foreign Subsidies Regulation poses new challenges for M&A in Europe

US investment into Europe evolving scrutiny of major FDI partner

Australian screening process placing FDI under greater scrutiny

CFIUS puts investors on notice of increased enforcement efforts

UK's national security and investment regime

Foreign investment monitor

Issue 6

May 2023

Freshfields

Welcome to our sixth Foreign investment monitor

In this edition, we look at the opportunities – and obstacles – presented by evolving FDI regimes around the world.

We examine the implications of recent developments in FDI regulatory regimes, shed light on the challenges faced by investors and offer guidance on successfully navigating them.

From the new challenges posed to M&A in Europe by the EU's Foreign Subsidies Regulation to the various approaches taken by different European authorities to US investors, we analyze the evolving landscape and provide insights on the impact of these changes.

In collaboration with Clayton Utz, one of our StrongerTogether partner firms, we feature an article looking at how Australia's expanded screening process will bring more transactions within the scope of its regime.

We also focus on the first-ever enforcement and penalty guidelines issued by the Committee on Foreign Investment in the United States (CFIUS) and discuss the Committee's attitude toward enforcement following their release. Finally, we look at recent developments surrounding the UK's wide-ranging national security and investment regime.

Join us as we delve into these crucial topics, providing the knowledge and insights necessary to navigate the complex global investment landscape. If you would like to discuss any FDI issue in more detail, we would be delighted to arrange a meeting. If there is something you'd like to see us cover in the next monitor, do let us know.

EU Foreign Subsidies Regulation poses new challenges for M&A in Europe

As of October 12, 2023, foreign investors will need to manage another layer of regulatory complexity to complete their investments in Europe: the Foreign Subsidies Regulation (FSR).

In addition to merger control and FDI screenings, under the FSR, the European Commission (Commission) will be looking into subsidies granted by non-EU countries to companies engaging in M&A within the EU. Although the Commission will have far-reaching powers under the FSR to investigate public tenders and any other situation involving foreign subsidies in the EU internal market, the scrutiny of transactions is expected to steal the limelight under the proposed new regime. Certain types of deal-heavy companies, such as private equity (PE) firms, pension funds and state-owned enterprises (SOEs), will be especially exposed to this unprecedented tool.

The FSR aims to close a perceived regulatory gap in order to level the playing field between the EU, where in principle state aid is prohibited, and third countries. The rationale of this new tool is that companies that have received public aid from third countries may have an undue competitive advantage compared to companies that have not had access to such state support, harming competition in the EU internal market.

The enforcement of the FSR with respect to M&A will be carried out similarly to merger control and FDI – parties will be required to notify a transaction to the regulator (here, the Commission) and will not be able to close it until it is cleared. However, each assessment is different. FDI screenings identify whether a particular investment could pose a risk to national security by leaving strategic activities in the hands of foreign investors. Merger control investigates potential reductions of competition as a direct result of increased levels of concentration. The FSR also protects competition, like merger control, but from another perspective: it targets distortions of the internal market caused by "distortive" foreign subsidies. Consequently, the procedures are complementary and might lead to different outcomes.

M&A deals that will need to be notified under the new regime

Companies will need to notify transactions signed after July 12, 2023 (the effective date of the FSR) and closed after October 12, 2023 involving an acquisition of control over a company, the establishment of a jointly controlled JV, or a merger if they fulfill two thresholds:

- The target, the JV or one of the merging parties is established in the EU (by, for example, having a subsidiary or a permanent business establishment in the EU) and generates a turnover of at least €500m in the EU, and
- The transaction parties – i.e., the target and acquirer, JV and parents, or both merging parties – have received combined "financial contributions" exceeding €50m from non-EU countries over the three previous years preceding the conclusion of the agreement, announcement of the public bid, or the acquisition of a controlling interest.

> Although the Commission will have far-reaching powers under the Foreign Subsidies Regulation to investigate public tenders and any other situation involving foreign subsidies in the EU internal market, the scrutiny of transactions is expected to steal the limelight under the proposed new regime.

While the first criterion is familiar to companies that have previously engaged with the EU merger control regime, the second is less familiar. Financial contribution is a very broad concept, catching not only direct grants, but also individual tax breaks, loans and contracts with public entities, as well as any provision or purchase of goods or services to or from any entity, whose actions are attributable to a non-EU government.

Making the regime even more onerous, commercial relations with public bodies on market terms count towards the financial contribution threshold – a type of activity that most companies will never have monitored. Contrary to the EU State aid regime, the concept of financial contribution, which triggers the notification obligation, does not require the recipient to have received a "benefit." Whether the recipient has received an individual benefit that distorts competition is only assessed during the Commission's investigation, following notification. Accordingly, absent further guidance, almost any ordinary course of business financial relationship with a government of a non-EU state – or even a private entity whose actions can be attributed to such third country – can technically result in a financial contribution, triggering the notification obligation.

Companies must be ready to disclose large amounts of information

Although the final notification form has not been yet approved by the Commission, the Draft Implementing Regulation published on February 6, 2023 suggests far-reaching disclosure requirements, which go beyond those of the EU Merger Regulation notification form and have no precedents under any similar regulatory tools.

Notably, if a company has received more than €4m of financial contributions from a single non-EU country in a year, it will be obliged to list line-by-line any individual contributions above €200,000. For each one of these contributions, the name of the granting entity, country, type of contribution and its amount must be provided. Note that, even if only financial contributions above €200,000 must be reported, all of them – no matter how small – must be monitored and count towards the €50m notification threshold set out above.

The Draft Implementing Regulation also requires other potentially burdensome disclosures regarding the transaction. For instance, the Commission calls for the sharing of copies of all due diligence analyses; or – if the transaction occurs in the context of a bidding process – the number of bidders that have participated, those who expressed an interest, or how many letters of intent and non-binding offers were received. Although waivers may be granted to excuse disclosure of information "not needed for assessment" or "not reasonably available," the decision to grant them fully lies within the discretion of the Commission. Part of this information is typically considered highly sensitive by sellers and other bidders and generally not in the possession of a winning bidder. It is unclear how the Commission will deal with this at a practical level – whether it will insist that the winning bidder procures the information from the seller after the auction process, whether it will obtain the information from the seller directly, or whether it will agree to a waiver request.

The process of assessing which financial contributions are problematic, and which are not

The submission of the notification commences an administrative procedure in two phases, aligned with EU merger control. The Commission will first assess whether a financial contribution is a foreign subsidy, i.e., whether it confers a benefit and is selective.

> Making the regime even more onerous, commercial relations with public bodies count towards the financial contribution threshold – a type of activity that most companies will never have monitored.

Secondly, it will analyze whether these foreign subsidies are "liable to improve the competitive position of an undertaking on the internal market" while negatively affecting competition in the internal market. Certain types of foreign subsidies are most likely to distort the internal market. This is the case of subsidies that directly facilitate a deal, as well as those granted to ailing undertakings and those in the form of an unlimited guarantee or export financing measures not in line with the OECD. Finally, the Commission can also balance the effects on competition against the potential positive effects of the subsidy.

If the Commission considers that the reported financial contributions do not confer a benefit, are not selective, or do not distort the internal market, it will issue a clearance decision within 25 working days following the notification. Otherwise, it will open an in-depth investigation for potentially another 90 working days (or 105, if remedies are proposed), and finalize it by either clearing the transaction with or without commitments or blocking the deal altogether.

Private equity firms, pension funds and SOEs will be especially affected

Frequent investors, such as PE firms, pension funds and SOEs, might be more exposed to the FSR than other investors. For PE firms, the screening for financial contributions across broad portfolios and multiple funds will be particularly burdensome. It cannot be excluded that the state-linked limited partner's LP investment is itself seen as a financial contribution received by the relevant PE firm, given the very broad concept described above. In addition, many portfolio companies will have arm's length financial relationships with non-EU states.

LP investments by pension funds and SOEs from non-EU Member States could potentially constitute financial contributions. Given the low €50m monetary threshold for financial contributions, transactions involving such LP investors would always trigger the notification requirement in case of M&A in the EU that exceeds the €500m EU turnover threshold.

Key takeaways to minimize the impact of the FSR on deals

- Companies engaging in economic activity within the EU need to start monitoring financial contributions as soon as possible. The Commission also has the authority to investigate foreign subsidies even outside the M&A context, so companies should be prepared to provide such information in a timely manner.
- Due diligence questionnaires must be extended to cover financial contributions, and SPAs should include additional provisions regarding cooperation on information disclosure and condition precedents.
- Actively engage with the Commission – especially on potential waivers – in order to prepare and to minimize information gathering and compliance costs.
- Consider the timing of ongoing deals - the notification obligation applies for deals signed after July 12 and closed after October 12.

With thanks to Freshfields' Merit Olthoff, Paul van den Berg, Andreas von Bonin and Justyna Smela for contributing this update.

US investment into Europe – evolving scrutiny of a major FDI partner

As foreign investment regimes mature across Europe, several trends in specific jurisdictions have emerged. For example, many EU member states took measures against Russia following the conflict in Ukraine.

China, too, faces significant scrutiny, with many EU states taking an increasingly cautious and conservative attitude to investments coming from China, especially those involving state-owned enterprises. Similar trends can be seen in the UK, which now has just over a year's experience of its new national security screening regime.

But what about the United States? The US is seen as a friendly power and even a close ally by most countries in Europe, so investments by American firms, as a general matter, are not subject to the most stringent controls and scrutiny. However, some clear differences between jurisdictions remain in terms of how they treat US investments.

FDI authorities tend not to treat US investors differently compared to the vast majority of countries that are considered non-hostile, with most concern reserved for investors from China, Russia, Iran and Belarus. "Any deal is always more sensitive with a Chinese investor than with a US investor, irrespective of what the target is doing," says Düsseldorf-based Dispute Resolution Partner Juliane Hilf. While there are exceptions in certain jurisdictions national authorities tend to "make no real distinction between EU and non-EU investors," remarks Paris-based Antitrust, Competition and Trade Partner Jérôme Philippe. "Obviously the US is a long-standing ally and is a state which is viewed as friendly." Rather, the analysis is transaction-specific and depends on the nature of the target, the target's relationship with the government, and the sensitivity of its contracts or informational capabilities.

Recent outcomes for US investors – prohibitions are rare, but mitigation remedies are quite common

The posture toward US investors is typically friendly across national authorities in Europe, and prohibitions of US investments are exceedingly rare. However, mitigation remedies are relatively common. Italy is a case in point: of the transactions prohibited since the creation of the Italian regime, all but one concerned China or Russia and none involved a US investor. Some transactions carried out by US investors have faced mitigation, although details of the measures imposed are not made public. Similarly, in Germany, despite no prohibitions of transactions by US investors, some have faced mitigation such as requirements dealing with access to information and specific data. As Juliane explains, "For example, it might be that only German citizens should have access, or that classified data should not be transferred."

Although prohibition by European authorities of US investments is very rare, it has occurred in exceptional cases. For example, among hundreds of cases in France, there has been one publicly announced prohibition of a transaction by a US investor, but that was in the context of a highly sensitive defense-related target.

The picture is similar in the UK. "For deals involving targets active in particularly sensitive sectors, such as defense, critical infrastructure and dual-use technologies or targets with sensitive government contracts, I wouldn't say there's any different treatment for US investors as compared to other non-UK investors," explains London-based Antitrust, Competition and Trade Counsel Sarah Jensen.

Sarah highlights that under the previous public interest regime, the UK government intervened in 16 deals on national security grounds over an 18-year period, eight of those deals involved US bidders. "None were prohibited, but all involved mitigations to protect information or strategic capabilities in defense or other sensitive sectors," says Sarah.

> FDI authorities tend not to treat US investors differently compared to the vast majority of countries that are considered non-hostile … the analysis is transaction-specific and depends on the nature of the target.

Under the current UK regime, the UK government has imposed final orders (mitigations or prohibitions) in 15 deals since January 2022, of which three have involved US bidders. "Again, no deals involving US acquirers have so far been blocked, but conditions have been imposed to protect sensitive information in defense or critical infrastructure-related businesses," says Sarah, "as well as continuity of supply in Ministry of Defence and government programs, and maintaining strategic capabilities and R&D in the UK." In terms of mitigation, UK regulators might require that UK citizens be on the board of particularly sensitive targets, Sarah says.

"I think the same would apply to US bidders as anyone else."

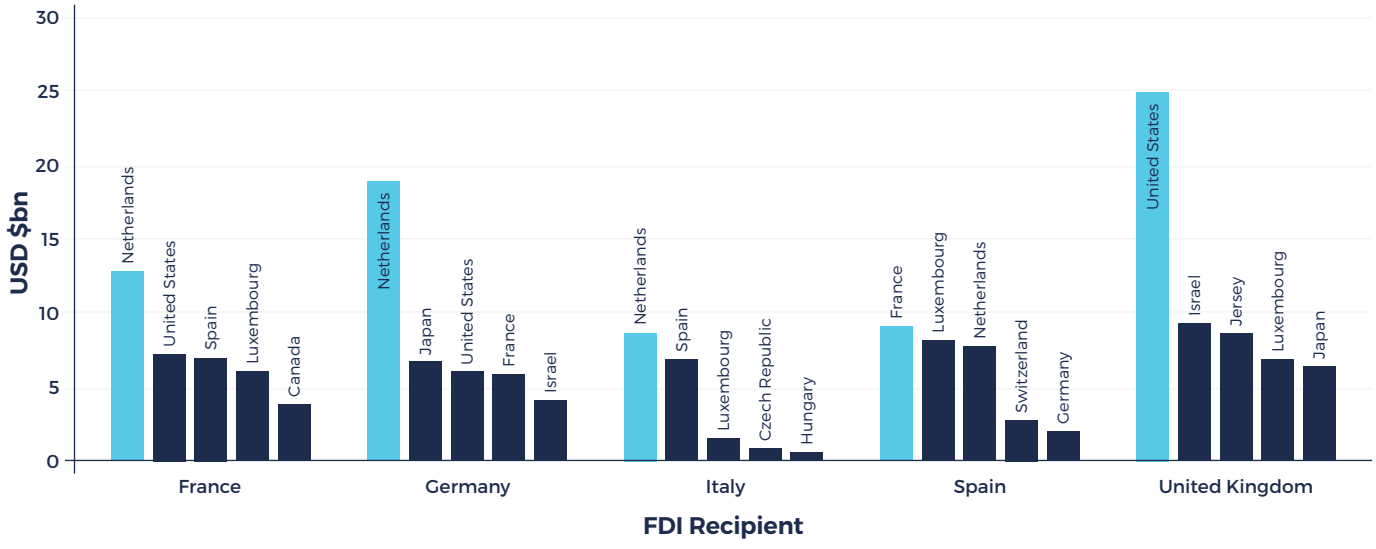
In Spain, "It is possible that the Spanish authorities approve a transaction, requiring the investor to commit to comply with labor laws, previous investment levels or other prudential regulations to protect national interest which is a very simple but effective condition," says Madrid-based Antitrust, Competition and Trade Counsel Enrique Carrera. Many authorities have required that the target should stay in its home country or requested commitments to retain local R&D capabilities or even the entire local business.

They may also require that management remain in the home country but, as Juliane explains, this depends on the sensitivity of the target with little regard to the investor's country of origin: the more sensitive the target business, the more obligations.

Disparity of outcome between European states?

While US investors will generally be viewed favorably across European jurisdictions, outcomes may still vary from jurisdiction to jurisdiction even on the same transaction.

Top 5 sources of FDI, 2021



Source: OECD · Includes equity, debt and reinvestment of earnings.

> Although prohibition by European authorities of US investments is very rare, it has occurred in exceptional cases.

In the EU, the Screening Mechanism has led to greater convergence between national authorities' theories of harm. But, as Juliane explains, decisions don't always come out the same way. Outcomes can vary widely, but "there might be good reasons for that" as a matter of both jurisdiction and substantive national security risk.

"Often there is a very valid reason why the outcome is different in different countries, typically that the target's activities are different," agrees Milan-based Antitrust, Competition and Trade Partner Ermelinda Spinelli. "For instance, when a US private equity buyer of an Italian engineering company notified the transaction, the Italian Prime Minister's Office actually declined jurisdiction even though remedies were imposed in France. But in France the target was a supplier to the public railway and in Italy it wasn't."

Such seemingly uneven treatment can also be due in part to the evolving nature of cooperation across EU countries, says Jérôme Philippe. "Member states don't necessarily have the tools to fix issues that emerge in another member state. And some deals that are notifiable in one country may not be notifiable in another country or may be declared 'out-of-scope.' Outcomes vary depending on the situation across various countries."

National interests as a driver of scrutiny

In addition to national security, economic independence and national interest are explicit or implicit considerations for FDI regimes in most European countries. These issues are often agnostic to the origin of the investor; they tend to be specific to the target itself, its industry, or even its workforce alone, all within its home country. When large players in high-scrutiny industries are American, increased consideration of national interest factors may disproportionately affect US firms. But, as Juliane points out, defining "national interest" and differentiating it from a purely economic interest can be difficult. "Being economically independent can also be seen as a national security interest, as we've seen during the war in Ukraine."

In Italy, for example, "there is increasing attention on the need to preserve employment levels and keep R&D and patents in the national territory, as shown by a very recent case where the Italian FDI authority imposed remedies in the white goods sector based precisely on such concerns," Ermelinda explains.

To take another example, Italy, Spain and many other European jurisdictions expanded the scope of their FDI regimes during the Covid pandemic. "The Italian regime is very broad and the Italian FDI authority enjoys a wide margin of discretion. General market practice is to be quite conservative and submit filings in case of uncertainty, or at least formally consult the authority," says Ermelinda. For its part, in 2020 Spain began to apply its rules for ex-EU investors to EU investors in response to low valuations of Spanish listed companies as an "anti-takeover shield" as defined by the Spanish media. "The idea was to stop foreign investors from acquiring Spain's 'crown jewels,'" Enrique says. But Spain is traditionally open to foreign investment and US investors are 'traditional customers' of Spain's FDI authorities."

In Germany, "there are trends as to which types of businesses the government focuses on," says Juliane. "During the pandemic, it was the health sector, then robotics was something they were very interested in, now it's more artificial intelligence, semiconductors, crypto and emerging digital areas. This might be more relevant for US investors because the big players are often US multinationals."

Treatment of financial investors

Financial investors from the United States should no longer expect their investments to fly under the radar of

> Few US investors are surprised at the scrutiny they face in Europe ... but the environment is changing, so they should take careful note of developments.

FDI authorities in Europe. Although they may not be treated differently from investors in other countries, scrutiny has increased across the board. For example, Germany tends to apply the same scrutiny to financial as to strategic investors, Juliane says, with authorities focusing on whether an investor is reliable, with concerns prompting further investigations into the ultimate beneficial owner. "Financial investors investing in a number of businesses can already be known to the authorities so actually raise fewer issues."

In the UK, financial investors should also expect similar treatment to other buyers. "Although some antitrust agencies are paying more attention to financial investors in merger reviews, the focus in national security reviews remains whether concerns can be mitigated through appropriate conditions which are tailored to the sensitivity or strategic nature of the target business," Sarah says. "Financial investors have been subject to mitigations under the previous and current UK regimes, but we haven't really seen any different treatment yet."

US financial investors should be prepared for authorities to look up through ownership chains to identify all players who may have influence over targets. Details required in filings differ between countries but powers to request further information can be extensive. For example, in the UK, details of passive interests held by limited partners (LPs) are not typically required upfront. "But we have seen cases where that type of information has been asked for," Sarah says.

There is no general rule requiring PE firms to disclose their LPs in Italy, but the authority "technically has the power to ask for very, very detailed information," Ermelinda says.

Meanwhile, in France, all private equity firms, not just those from the US, should be expected to have to disclose their LPs if they reach thresholds, in large part due to concerns over changes in ownership.

Outlook and strategy

Few US investors are surprised at the scrutiny of US investment in Europe, especially given the often-strict stance taken by the Committee on Foreign Investment in the United States to investments coming in the opposite direction. Nevertheless, the environment is changing, so investors should take careful note of recent and upcoming developments.

With increased levels of scrutiny under rapidly developing regimes, it is even more important to seek advice early to identify potential filings and concerns, and ensure that notification and review processes are as efficient and streamlined as possible. "It's about identifying where filings are needed or advisable, anticipating the issues that are likely to arise in each country, providing the necessary contractual protections for parties and implementing proactive strategies that bridge commercial rationales with national security concerns," says Sarah. Staying close to the authorities and understanding the trends and developments which are driving reviews remain key to deal certainty.

With thanks to Freshfields' Juliane Hilf, Jérôme Philippe, Ermelinda Spinelli, Enrique Carrera, Sarah Jensen and Petya Katsarska for their contributions to this update.

An expanded Australian screening process placing FDI under greater scrutiny

Contributed by Geoff Hoffman and Kirsten Webb at Clayton Utz, which is part of the Freshfields StrongerTogether network.

With a strong economy, stable political environment and proximity to key regional markets, Australia is highly attractive to foreign investors. Indeed, foreign investment is critical to the country's long-term economic success. Nevertheless, in recent years Australia has introduced a number of reforms that have resulted in a foreign direct investment (FDI) regime that is much more extensive in reach than ever and covers a broader range of transactions.

This expansion is partly due to concerns over a global socio-economic environment that is less stable than in previous years. Further, rapid technological advancement coupled with geopolitical and security challenges have seen heightened concern around cyber-attacks, which potentially affect not just defense assets but also major transport infrastructure, the banking system and a range of other sectors. In this respect, the Australian approach towards FDI reflects the wider global landscape in which many countries have reviewed and strengthened their FDI frameworks.

Crucially, amendments to the Security of Critical Infrastructure Act 2018 have expanded the scope of what is considered a "national security business" while simultaneously lowering the threshold for coverage under the Act. Previously, the definition only covered large electricity, gas, water and port infrastructure assets, as well as traditional defense assets. The new definition now covers industry sectors such as telecommunications, food and grocery, financial services and banking, and higher education and research to name a few. As a result, investments of 10 percent or more in the newly expanded list of industries are subject to a mandatory, suspensory filing requirement, regardless of the value of the investment. Foreign investors seeking to acquire businesses in these newly covered sectors will need to evaluate – and factor into their transaction timelines – the potential need to obtain Foreign Investment Review Board (FIRB) approval and, if so, when to approach FIRB.

Australian reforms have introduced significant changes to the filing fee regime, which is complex and subject to multiple exceptions and rules for specific situations. For foreign investors looking to acquire an interest in Australian entities, assets or land, the application fees have doubled and can reach over A$1m for acquisitions of more than A$2bn. There is also a more assertive enforcement function within FIRB with significantly increased penalties for failures to notify and obtain required approvals, and investment in an expanded enforcement capability.

Unsurprisingly, the impact of these reforms has been significant. The broadened definition of national security business and the accompanying reduction in investment threshold for triggering the FIRB approval requirement have resulted in an increase in applications to FIRB for transaction approval. The effect is that the regime now requires review and approval of even very small and non-substantive transactions involving national security businesses, including indirect changes of ownership arising from offshore transactions. According to FIRB statistics, in the six months to December 2022, newly covered transactions subject to the mandatory regime accounted for nearly 10 percent of all notifications. The average value of those marginal transactions was approximately A$58m, or about 40 percent of the average value for all other transactions for which approval was sought (which is about A$150m).

> Recent reforms in Australia have expanded the scope of what is considered a 'national security business.'

Merger Control Interplay

The expanded scope of coverage also highlights the interplay between FIRB and the Australian Competition and Consumer Commission (ACCC), which administers the merger control regime. If a transaction is likely to face antitrust scrutiny, investors and companies must think very closely at the outset of the transaction about whether FIRB approval is mandatory or merely advisable. The ACCC cannot block transactions on its own authority (as the European Commission can), yet it can apply to the court to do so (as the US agencies also must). However, if a transaction is subject to FIRB approval, FIRB will not approve the transaction if the ACCC has concerns. This results in FIRB approval becoming a de facto instrumentality for the ACCC to block transactions without ACCC approval.

In global M&A deals where the target has an Australian subsidiary or business, it is possible that the transaction will fall within the voluntary (as opposed to mandatory) FIRB notification regime. This regime provides that parties can complete the transaction without prior approval but gives the Treasurer the right to unwind a transaction if they subsequently determine that the transaction is contrary to the national interest. Therefore, where the parties are seeking regulatory approvals in various jurisdictions for such transactions, it is generally considered prudent to also file in Australia under the voluntary notification regime.

However, if a transaction falls into the voluntarily notifiable category, once the parties have notified FIRB, they cannot complete the transaction until approval is provided – and, as explained above, if the ACCC has concerns with the transaction, they can effectively block the transaction unless they are satisfied.

Therefore, when subject only to the voluntary regime, companies may wish to consider not notifying FIRB and completing the transaction, leaving them free to pursue any strategy they wish from an ACCC perspective.

Eyes on Chinese investors as data security concerns mount

In line with developments elsewhere in the world, Australia's FDI reforms have occurred in parallel with the perceived shift in China's position, leading to increased scrutiny of Chinese investors. Ordinarily, transactions which will not obtain approval are withdrawn rather than publicly blocked. Nonetheless, in recent years, we have seen some public prohibitions by FIRB of acquisitions by entities with Chinese interests, such as a lease over the electricity transmission network in New South Wales and South Australia. While the government is careful not to overtly single out individual countries as the subject of scrutiny, companies perceived to be the subject of some form of state ownership or control draw the most scrutiny. China has many state-affiliated companies, and it remains one of the top five foreign investors in Australia.

Strategic investors are subject to closer scrutiny by FIRB than financial investors if they already have a presence in Australia. By contrast, financial investors are perceived as being more friendly than strategics from a foreign investment perspective. That said, private equity funds with large foreign government investors, including sovereign wealth fund investors, are effectively treated as foreign government investors and draw corresponding scrutiny from FIRB. Australia's regime reserves the closest scrutiny for investments by foreign government investors.

Data security has been a longstanding concern for the Australian government when reviewing foreign investments. This trend continues to be a significant factor in the government's scrutiny of offshore transactions. For example, if a target Australian business has databases containing personal details of Australian citizens, or government contracts with access to sensitive government data, the transaction will be subject to more stringent scrutiny. As a condition of approval, FIRB may impose conditions concerning the handling of that data and require independent audits to monitor compliance.

Further changes on the way

The Australian government is introducing the new Register of Foreign Ownership of Australian Assets from 1 July 2023. We expect the new register to impact foreign investors both directly and indirectly. The new reporting regime will both require companies to have new internal systems to enable compliance and require reporting of disposals of interests, necessitating a significant change in the approach to FIRB and requiring significant investment in processes and systems.

CFIUS puts investors on notice of increased enforcement efforts with first ever enforcement and penalty guidelines

Historically, the Committee on Foreign Investment in the United States (CFIUS) had limited resources dedicated to monitoring and enforcement of mitigation agreements.

The Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018 provided additional resources for CFIUS to build out its monitoring and enforcement capabilities. Following FIRMMA's passage, however, CFIUS focused first on implementing provisions that had statutory deadlines, such as issuing regulations for a mandatory notification regime. Thus, prior to 2022, CFIUS had issued only two penalty notices, each of which entailed relatively modest monetary fines ($1m or less) for egregious conduct. Looking ahead, things could significantly change.

With the FIRRMA regulations fully in force, CFIUS is working to further develop its monitoring and enforcement framework. On October 20, 2022, the US Department of the Treasury (Treasury), as chair of CFIUS, released the first-ever CFIUS Enforcement and Penalty Guidelines (Guidelines). Internal drafts of the Guidelines were prepared as early as 2017, but CFIUS's focus was subsequently diverted to passage and then implementation of FIRRMA.

The Guidelines are not revolutionary on their face, insofar as they reflect factors that are common sense and generally consistent with enforcement guidelines under other similar national security regulatory schemes. Instead, the Guidelines are notable in what they portend—that CFIUS is prepared to wield the stick that Congress first gave to CFIUS in 2008 (authority to impose penalties of $250,000 or the value of the transaction, whichever is greater) and sharpened with FIRRMA in 2018 (e.g., penalty authority for failure to make a required filing). Indeed, in the press release that accompanied the Guidelines, Assistant Secretary of the Treasury for Investment Security Paul Rosen, the political head of CFIUS, stated unequivocally that "compliance with CFIUS mitigation agreements is not optional, and the Committee will not hesitate to use all of its tools and take enforcement action to ensure prompt compliance and remediation, including through the use of civil monetary penalties and other remedies."

Having built out a robust monitoring and enforcement capability as part of the implementation of FIRRMA, and having telegraphed its intentions by issuing the Guidelines, CFIUS has already begun to step up enforcement against transaction parties that fail to make mandatory filings or that violate the terms of the National Security Agreements (NSAs) that form the basis for CFIUS to clear certain transactions that otherwise pose national security risks. Indeed, in April 2023, Rosen announced that CFIUS had imposed the first penalties following the issuance of the Guidelines. He noted that information about such penalties would be published in batches on a periodic basis, and we expect that the penalties may be described in the next CFIUS Annual Report, likely to be published over the summer.

> The CFIUS Enforcement and Penalty Guidelines are not revolutionary on their face but are notable in what they portend: Congress has sharpened the enforcement stick that it gave to CFIUS in 2008 – and CFIUS is prepared to wield it.

Why might investors be faced with a CFIUS enforcement action?

- **Failure to file a mandatory declaration or notice.** CFIUS's mandatory filing rules—particularly those related to critical technologies—require a combination of technical and legal analysis that can be complex to apply. However, getting this analysis right is critical because liability for failure to file falls on both buyer and seller.
- **Noncompliance with CFIUS mitigation.** This might arise in any number of ways:
  - Willful misconduct or negligence, such as failure to take steps to operationalize the NSA, including agreement to NSA terms that the company reasonably knew it would not be able to abide by.
  - Changed or unexpected circumstances. Despite parties' good faith intention of complying with an NSA, even the most meticulously drafted NSA cannot foresee all future circumstances that will arise throughout its life, and it is possible that full compliance may not be feasible in some instances. Notably, however, CFIUS officials have publicly stated that the high cost of compliance, even if material to transaction value or discovered after closing, is not such a circumstance. The obligation falls on transaction parties to make assessments of burden in advance of their entry into mitigation.
  - Differences of interpretation. If the CFIUS Monitoring Agencies (CMAs) that administer the NSA differ with the parties on a question of interpretation, the CMAs may determine that a company's actions taken in reliance on its own interpretation, even if formed reasonably and in good faith, may nonetheless constitute noncompliance.
- **Making a material misstatement, omission, or false certification.** Ensuring the accuracy and completeness of all information provided to CFIUS during the course of a filing and in connection with an NSA is obviously essential for compliance. However, the Guidelines note that penalties can be assessed for misstatements or omissions in information provided during informal consultations as well. It is also important to note that, in addition to civil penalties, a material misstatement or omission can serve as the predicate for CFIUS to reverse a grant of safe harbor and reopen a review.

Guidelines: The truth might set you free … or at least reduce the amount of your penalty.

CFIUS has discretion when determining the amount of a penalty or whether to assess a penalty at all. Moreover, it does not view all violations as being equally severe, and it will generally attempt to calibrate the penalty to the facts and circumstances surrounding a violation. The Guidelines identify six high-level **aggravating and mitigating factors** that CFIUS considers when deciding whether to assess a penalty and the amount of the penalty. Transaction parties can use these factors as a guide for taking proactive steps both before and after a violation occurs to limit the amount of any corresponding penalty. Below are the factors identified in the Guidelines along with key takeaways from each:

> CFIUS has already begun to step up enforcement against transaction parties that fail to make mandatory filings or that violate the terms of National Security Agreements.

1. **Accountability and future compliance.** Is the enforcement action sufficient to deter bad behavior and incentivize future compliance? For example, a penalty that is large enough to get the attention of a small company might be a rounding error for a multibillion-dollar company.
2. **Harm.** To what extent did the violation impair US national security? A violation of a provision that is core to the agreement, or a violation that actually results in the harm that the agreement was intended to protect against, is more likely to draw stiffer enforcement action.
3. **Negligence, awareness, and intent:** There are two components to this factor. First, was the violation the result of simple negligence, gross negligence, intentional action, or willfulness?

   Second, who knew about the violation, who should have known about it, and was there any attempt to conceal it? Ignorance is no excuse if, in CFIUS's estimation, the person claiming ignorance should have known about the requirement. Worse still, there is no quicker or surer way to transform an act of simple negligence into an act of willfulness than to try to hide it from CFIUS.
4. **Persistence and timing.** How long before the violation was reported and/or remediated and how many times did it occur? Generally speaking, one-off violations will be granted more leniency than repeated violations of the same magnitude. In the case of an NSA violation, failure to report a known or suspected violation (once discovered) within the time period stipulated in the NSA will almost always be an aggravating factor (and, indeed, could also be considered a separate violation of the terms of the NSA). In the case of a failure to make a mandatory filing, CFIUS will consider the date of the transaction and the date it was self-reported or discovered by CFIUS.
5. **Response and remediation.** Did the transaction parties self-disclose, provide required information, cooperate fully, and take prompt and effective remedial action? Self-disclosure is the most important component of this factor; if CFIUS comes knocking, they are probably bringing a penalty with them. The content of the self-disclosure also matters. CFIUS wants as much information as possible about the violation, as soon as possible, including when supplemental information becomes available or when CFIUS asks questions. Stonewalling will not be viewed favorably.

   Taking proactive, immediate remedial action is a mitigating factor, especially if it can be shown that the remediation was effective. Standardized forms and processes used to report and investigate violations, performing root cause analyses, assessing consequences, and document remediation efforts can be very useful for demonstrating effective response and remediation. That said, transaction parties should not wait to self-disclose a violation until after remediation efforts are complete on the belief that the CMAs will be pleased to be presented with a problem that has already been solved. If remediation and mandatory reporting timelines conflict, parties to an NSA should timely report the violation, describe the ongoing remediation efforts, and continually update the CMAs until the remediation efforts have concluded.
6. **Sophistication and record of compliance.** Do the transaction parties have strong track record with the Committee and/or a general culture of compliance? The cornerstone of any successful CFIUS mitigation agreement is trust between the CMAs and the transaction parties. The most common basis for this trust is a long and successful track record of filing with the Committee and/or implementing one or more NSAs. Companies without this kind of history with CFIUS can begin building trust through candor in interactions with the Committee, demonstrating buy-in from senior leadership, and devoting sufficient resources to compliance and training.

> CFIUS does not view all violations as being equally severe, and it will generally attempt to calibrate the penalty to the facts and circumstances surrounding a violation.

Aside from the mitigating and aggravating factors themselves are two takeaways for investors:

CFIUS is willing to listen to your side of the story when determining how to respond to a violation. If CFIUS finds a violation, it will first send a notice of a determination of non-compliance. If it determines that a penalty is warranted, it will also send a notice of a penalty, including the amount, a description of the conduct being penalized, and the legal basis for the penalty. The recipient then has an opportunity to submit a petition for reconsideration that includes any defense, justification, explanation, or mitigating factors. If no petition is submitted (or the petition is not timely), CFIUS will issue a final penalty determination. If a petition is timely submitted, CFIUS will consider the petition before issuing its final penalty determination. Even if the recipient of a penalty notice believes it is unlikely that CFIUS will ultimately reconsider the penalty, it may nonetheless be worthwhile to submit a petition to correct any erroneous facts in the notice, ensure that CFIUS has all relevant facts, and generally try to manage the relationship with the Committee.

It might not always seem like it, but the CMAs generally view themselves as your partners in success, not your enemy. CFIUS's mission is to protect national security in the context of the open investment policy of the United States. If CFIUS has cleared a transaction pursuant to an NSA, it wants both the mitigation to succeed in protecting national security and the transaction to succeed in delivering the anticipated value to the parties. As such, it generally views the relationship between the CMAs and the parties to an NSA as more cooperative than adversarial, and it encourages the parties to take the same view.

With thanks to Freshfields' Aimen Mir, Christine Laciak, Colin Costello and Tim Swartz for contributing this update.

The UK's national security and investment regime – key developments as practice continues to evolve

Since our last update on the UK's National Security & Investment (NSI) regime in November 2022, not only has the NSI regime celebrated its first birthday, but there have been several significant developments in relation to how the UK government is using its wide-ranging powers to intervene in deals on national security grounds, and how investors should approach the regime when planning and executing deals.

Five more deals blocked, unwound or subject to remedies

Over the last five months (December 2022 – April 2023):

- one more deal has been blocked (the proposed acquisition of HiLight Research by SiLight, a Shanghai semiconductor company) and another has been ordered to be unwound (LetterOne's acquisition of Upp, a regional broadband provider), reinforcing a continuing trend of all prohibitions so far having Chinese or Russian links. The decision to force the sale of Upp is under appeal (see below); and
- three more deals have had remedies imposed to protect sensitive information and/or maintain continuity of supply. These span a range of acquirer nationalities (China, the US and Germany) and sensitive sectors (communications, energy and defense).

These deals take the total number of remedy cases in the first 16 months of the regime to 15, which is noticeably higher than the UK government's original expectations. Back in November 2020, the government estimated 10 remedy cases and 1,000-1,830 notifications per year. In practice, 2022 saw the UK government impose remedies in 14 cases and review about 800 deals. Given the current geopolitical environment, this rate of intervention and mitigation is expected to continue.

Notwithstanding these statistics, businesses should be aware that a decision by the UK government to "call in" a transaction for a full national security assessment is not necessarily a signal that remedies are required; call-in cases can (and do) get cleared without mitigation. This position contrasts with the previous regime under the Enterprise Act 2002 where, if the UK government had issued an intervention notice on national security grounds, it was highly likely that a review would end with remedies.

A new "decision maker" in government

In February 2023, the Investment Security Unit (ISU) moved from the now-slimmed-down Department for Business to the Cabinet Office. The "decision maker" is now the Secretary of State in the Cabinet Office (Oliver Dowden MP), rather than the Secretary of State for Business. Although some critics suggested this move would politicize the ISU and its work, other stakeholders viewed it as a natural move back to where the unit was originally incubated. Being at the heart of government, the ISU may be better placed to corral other government departments for the sector expertise which is essential for NSI reviews, while benefiting from governmental national security and intelligence expertise which is concentrated in the Cabinet Office. The move also allows for greater oversight from the Prime Minister's office as national security is known to be one of Rishi Sunak's key priorities.

> In the UK, businesses should expect a continued focus on frontier technologies such as quantum computing, semiconductors and artificial intelligence, as well as defense and critical infrastructure.

One of Mr. Dowden's first steps in his new role was to respond to business concerns about the lack of transparency over the regime by publishing new guidance and engaging in roundtable discussions with companies to provide more information about what to expect during reviews (see further below). There has not yet been any indication of the move impacting the outcome of reviews, although this is clearly a rapidly developing and politically charged area.

Developments in the UK government's national security policy

The Integrated Review Refresh (published in March 2023) gives further indications of the types of deals which will attract scrutiny. Priorities include strengthening the UK's domestic resilience in response to the "epoch defining challenge" that is China, while also protecting national security from the increased threats posed by Russia and Iran and growing cooperation between those states. As the head of the UK's National Cyber Security Centre said recently, the UK and its allies cannot afford to be complacent over the "dramatic rise of China as a technology superpower."

Businesses should therefore expect a continued focus on frontier technologies such as quantum computing, semiconductors and artificial intelligence, as well as defense and critical infrastructure. And despite the clear focus on China and Russia, investments from traditional allies will continue to be scrutinized if there is a need to protect sensitive information, assets and/or activities in the UK irrespective of the acquirer's nationality.

Pressure on the ISU to improve its processes and increase transparency

The ISU has come under substantial pressure to improve communication with parties during reviews and increase transparency for the market. Concerns have come from all quarters including evidence given to the Business, Energy and Industrial Strategy (BEIS) Select Committee during its inquiry into information sharing by the ISU (February/March 2023), parties and their advisors, and thinktanks including the Tony Blair Institute for Global Change.

Already we have seen the ISU take some steps to improve communication with parties (e.g. more regular calls during reviews) and, in late April 2023, the UK government updated the NSI Guidance (previously updated in July 2022), building on stakeholder feedback on the NSI process to date. This new guidance provides more clarity on some important procedural aspects of the regime, including:

- **When to notify:** the ISU generally considers that it is appropriate to notify when there is a "good faith intention to proceed," which might be demonstrated by heads of terms, financing arrangements, board level consideration or a public announcement of a public bid. Parties may be able to notify earlier if there are "good reasons" for doing so, but caution should be exercised before notifying too early given the risks of notifications being rejected, further information requests or changes to the transaction which may count as separate trigger events.
- **Whether to notify:** the ISU has said that parties may seek a view on whether an acquisition is notifiable if there is "significant uncertainty" about whether or not a target's activities fall within one of the 17 mandatory notification sectors. Views are only likely if parties can provide sufficient details about the transaction and why there is uncertainty over whether it falls within scope of the regime. This is nevertheless a very welcome move given the technical nature of many of the sector definitions and calls for the ISU to provide more informal guidance to parties, as they did before the regime came into force.

> Despite the clear focus on China and Russia, investments from traditional allies will continue to be scrutinized if there is a need to protect sensitive information, assets and/or activities in the UK irrespective of the acquirer's nationality.

- **Dealing with financial distress:** the new guidance sets out the evidence parties are expected to provide to demonstrate that an entity is in material financial distress and that the ISU should therefore expedite its review process.

The updated guidance also provides more detail on interim orders (which may be issued to prevent or reverse actions by the parties during the assessment period), information and attendance notices (and their impact on review timelines) and how the ISU engages with parties if mitigation (remedies or prohibition) is being considered.

On-going reviews and updates to the ISU's procedures are expected as the UK government continues to balance the need to show that the UK is open for business and investment whilst protecting its national security. Further scrutiny is also expected following the **memorandum of understanding agreed in March 2023** which gives the BEIS Select Committee (and specifically the National Security and Investment Sub-Committee) access to the information required to scrutinize the ISU. This is likely to result in more on-going oversight and opportunities for stakeholders to give oral and written evidence to improve the regime's workability.

Watch this space

Looking ahead, several developments over the coming months will be key in shaping the UK's NSI regime and users' experience of it:

- **The first judicial reviews of (prohibition) final orders.** The High Court is set to hear judicial reviews for Nexperia/Newport Wafer Fab (prohibited 16 November 2022) and L1T/Upp Corporation (prohibited 19 December 2022). Although limited details of the UK government's decision-making are expected to be made public, key issues are likely to include: (i) the UK government's level of discretion when determining whether a transaction poses a risk to national security; (ii) the reasonableness and proportionality of the prohibitions (e.g. whether less restrictive remedies would have been more appropriate to mitigate the risks); and (iii) whether due process was followed (e.g. whether the UK government complied with its obligations to consider representations on possible remedies and to allow parties sufficient opportunity to make such representations).
- **The ISU's first full annual report due in June 2023.** As the first annual report covered only the first three months of the regime's existence, this year's edition (1 April 2022-31 March 2023) should provide more insights on overall trends in terms of notifications and timings of reviews and the sectors of the economy which are generating the most interest.
- **Policy developments.** In the next few months, the UK government is expected to publish plans to support and grow capabilities and technologies that are of strategic importance to the UK, including the UK's semiconductor sector, and a UK Supply Chains and Import Strategy to strengthen resilience in critical sectors. Businesses looking to buy or sell in the affected sectors should pay close attention to what these strategies, combined with the NSI regime, will mean for any pipeline sales/acquisitions, including their likelihood of success.
- **General Election run-up.** As we edge closer to the next UK general election (rumored to be planned for late 2024), there will be an increasing focus on any policy shifts or statements from either of the major political parties in relation to foreign ownership of strategic assets or how to protect the UK's national and economic security whilst encouraging vital foreign investment. Longer term, such policies will shape the future direction of the regime.

We will report further on these developments in future updates to the Foreign investment monitor, so please watch this space.

With thanks to Freshfields' Michele Davis, Sarah Jensen and Iona Crawford for contributing this update.

freshfields.com