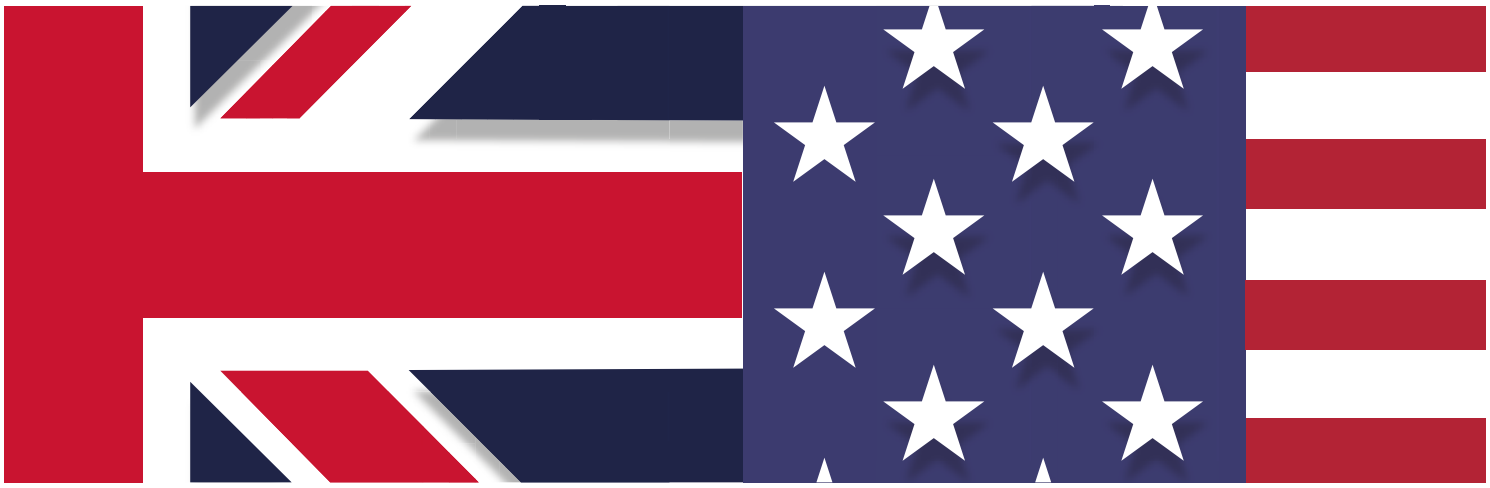


The UK-US Regulatory Relationship

A study into the UK-US regulatory market access barriers

Foreign Investment Screening and Data Privacy Regulation

CITY OF LONDON

The City of London Corporation

Our vision
The City of London Corporation is the governing body of the Square Mile dedicated to a vibrant and thriving City, supporting a diverse and sustainable London within a globally-successful UK.

We aim to:
- Contribute to a flourishing society
- Support a thriving economy
- Shape outstanding environments

By strengthening the connections, capacity and character of the City, London and the UK for the benefit of people who live, work and visit here.

Our reach extends far beyond the Square Mile's boundaries and across private, public and voluntary sector responsibilities. This, along with our independent and non-party political voice and convening power, enables us to promote the interests of people and organisations across London and the UK and play a valued role on the world stage.

Supporting the UK-wide financial and professional services industry

The financial and professional services industry is key to the ongoing prosperity of the UK. It provides exports more than double those of any other sector, and significant contributions to employment, tax and productivity – across the country. The City of London Corporation works with partners in industry and local and national governments across the UK, to keep the UK competitive into the future: nurturing innovative sectors, securing the best environment for firms to thrive, supporting inclusive and sustainable growth, and showcasing the sector's UK-wide offer. We work to promote the industry to overseas markets: attracting and retaining investment, building partnerships and sharing expertise to secure long-term, worldwide trading relationships.

CITY OF LONDON

December 2020

Contents

Executive Summary

Against the backdrop of ongoing Free Trade Agreement (FTA) negotiations, the UK and US have an opportunity to develop a new and enhanced bilateral regulatory relationship in Financial and Professional Services (FPS).

Both countries already enjoy a robust, trust-based regulatory relationship which has underpinned meaningful collaboration. Such cooperation allows for more compatible and consistent regulatory outcomes which, in turn, provide a foundation for job creation and growth across the UK and US economies.

The formation of the US-UK Financial Regulatory Working Group (FRWG) in 2018 provides a potential mechanism for further enhancing bilateral regulatory and supervisory cooperation. Realising this potential will require the FRWG, or an alternative structure, developing a forward-looking mandate complete with a long-term vision for regulatory alignment.

This paper is the first in a 'UK-US Regulatory Relationship' series which will seek to develop this vision. The research aims to identify and contextualise the key market access barriers facing UK and US firms doing cross-border business or seeking to do cross-border business in FPS. The paper also provides recommendations for how UK-US regulatory and supervisory cooperation could address these issues to the benefit of cross-border FPS activity and, ultimately, consumers on both sides of the Atlantic. Eventually, this series of reports will be combined to provide a holistic image of the UK-US market access landscape.

Over 2020-2021, enhanced and informed by the City of London Corporation's extensive programme of US activity, we will publish a series of granular studies. These will cover the regulatory market access barriers facing banking, asset management, insurance and market infrastructure firms, and a series of cross-cutting frictions impacting bilateral trade across the waterfront.

This will be a collaborative project based on cooperation with stakeholders across the FPS spectrum. As we continue with this research, we welcome comments and thoughts on future priorities for further study.

This paper focuses specifically on two of the key cross-cutting issues:

- The recent implementation of the Foreign Investment Risk Review Act (FIRRMA) and its implications for foreign investment.
- The firm-level impacts of overlapping regulatory regimes in the area of data privacy.

Key recommendations

Technology: CFIUS-FIRRMA

Though the UK is currently exempt from the Committee on Foreign Investment in the United States (CFIUS) Foreign Investment Risk Review Modernisation Act of 2018 (FIRRMA) regulatory changes, it will need to establish a robust process to assess foreign investments to remain so. The UK Government has recently presented the UK National Security and Investment Bill to Parliament, but should continue to work closely with firms to further develop this regime and seek clarity from US regulators on how to effectively maintain this exemption.

While exemption of the UK for most provisions does provide a reprieve, it could be strengthened through extended certainty. The UK and US are already partners in national security through the Five Eyes partnership and already share significant amounts of data between themselves. This should not only limit the national security concerns which CFIUS is meant to manage, but also illustrates the strong regulatory and governmental ties between the two countries which should be encouraged.

The UK data regime surrounding personal data provides stronger protections to individuals than the US federal regime. This means that even when data is managed by the UK there should be limited risk that it would be utilised in a way that could constitute a national security risk for the US. This will continue to be a crucial angle for the UK to emphasise in discussions with US regulators concerning the appropriate protection of personal data required under CFIUS review.

The CFIUS review process is viewed as unpredictable and difficult to respond to by firms. The review process generally lacks transparency and there is often no burden of proof for when CFIUS decides to block FDI. There is wide scope for CFIUS to act through unilateral action, which operates in a distinctly different way to other more familiar judicial procedures firms may have experienced. Industry would find value in an increase in transparency in both process and final decision. This could be done through increased communication with the firms involved.

continues...

Data regulation

UK firms would benefit from more clarity regarding assessment of appropriate data protection and the General Data Protection Regulation (GDPR)-Privacy Shield intersection to ensure compliance within this complex web of regulations and court orders. Regulators and authorities on both sides of the Atlantic continue to work to resolve the issues brought about due to the impact of Schrems II on Privacy Shield.

US regulators remain uncertain of the effects of GDPR on their ability to obtain the necessary data and information to provide appropriate supervision of UK firms operating within the US. This is illustrated through the recent resolution of the SEC moratorium on investment advisor registration due to perceived conflict between the US Advisors Act of 1940 and GDPR. UK regulators and policymakers should work to continue to have open dialogue with their US counterparts to provide assurances that this should not be a concern.

In the US, there is no single data regulation and protection regime. There exists instead a patchwork of state-level data regulation structures. This lack of US federal regulation in data and the various interactions and differences between state rules regarding data places an unnecessary regulatory burden on UK firms. The UK should advocate in support of an overarching structure and guidance for regulation.

Broader regulatory cooperation between the US and the UK should be forward facing and enable discussions of potential future regulatory issues which could create unintentional barriers to market access. By understanding the responsible regulators on both sides of the Atlantic and ensuring appropriate dialogue between them, this can be avoided. Through establishing and strengthening appropriate regulatory dialogue on specific issue areas and for specific aspects of the financial and professional services sectors, both sides can better understand the regulatory reach, aims, and concerns of their counterparts.

Introduction

The UK and the US enjoy a deep, long-standing economic relationship based on more than commercial incentives. Both are market-oriented economies and home to the world's two leading financial centres. Strong trust-based relationships exist between respective financial regulators and institutions. The October 2020 MoU committing the US Commodity Futures Trading Commission (CFTC) and the UK Bank of England to joint supervision and oversight of cross-border clearing operations is the latest example.[1]

These and other factors underpin a thriving economic relationship: The US is the UK's largest single export market and both the US and UK are each other's largest sources of foreign direct investment. US investors are the largest international employers in UK financial services, covering banking, asset management, insurance and law. Developing a still more efficient and integrated relationship will bring opportunities to build on these strong foundations.

For the UK Government, recalibrating UK-US relations is a top priority post-Brexit. This brings opportunities to enhance the bilateral relationship in FPS. As most existing barriers to cross-border FPS trade and investment are regulatory in nature, the FPS industry has advocated pursuit of a dual strategy which holistically balances the potential benefits of a Free Trade Agreement and regulatory cooperation through the British American Finance Alliance.[2]

A focus on the latter has the capacity to deliver meaningful gains in the near term. Enhanced bilateral regulatory cooperation should identify and remove existing market access barriers, overlaps and frictions; ensure more consistent and compatible regulatory outcomes into the future; underpin greater bilateral collaboration in the international policymaking arena; all combining to support cross-border investment, growth and job creation across the entire UK-US economies.

The COVID-19 crisis strengthens the case for greater UK-US regulatory cooperation. Indeed, such coordination in the early days of the crisis enabled swift and aligned regulatory action which kept global markets functioning. Minimising market fragmentation as global economies negotiate further national lockdowns and re-openings will be crucial. UK-US regulatory dialogue will be an important element of the recovery and ensuring the limitation of market fragmentation. Furthermore, COVID-19 has highlighted the importance of sound regulatory practices in key policy areas such as prudential standards. Greater systematic cooperation in these areas will ensure a more robust global recovery.

1 CFTC and BoE sign new MOU for Supervision of Cross-Border Clearing Organizations **https://www.cftc.gov/PressRoom/PressReleases/8289-20**

2 British American Finance Alliance: Scoping paper on formalizing UK-US regulatory dialogue - **https://www.sifma.org/wp-content/uploads/2020/09/British-American-Finance-Alliance-Scoping-paper-on-formalizing-UK-U.S.-regulatory-dialogue.pdf**

Technology: Implications stemming from changes to the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA)

Relevant legislation: Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA)

Main Takeaways:

Implemented in early 2020, the Foreign Investment Risk Review Act (FIRRMA) broadens the Committee on Foreign Investment in the United States' (CFIUS) authority to take regulatory action in relation to foreign investment.

The UK is currently exempt from these changes but will need to establish a robust process to assess foreign investments to remain so. The UK Government has recently presented the UK National Security and Investment Bill to Parliament, but should continue to work closely with firms to further develop this regime and seek clarity from US regulators on how to effectively maintain this exemption.

While exemption of the UK for most provisions does provide a reprieve, it could be strengthened through extended certainty. The UK and US are already partners in national security through the Five Eyes partnership and already share significant amounts of data between themselves. This should not only limit the national security concerns which CFIUS is meant to manage, but also illustrates the strong regulatory and governmental ties between the two countries which should be encouraged.

Recent rule changes have the potential to block future partnerships between banks and tech companies. This could be due to firm concerns over CFIUS reviews or by direct CFIUS intervention in foreign investments into firms which handle personal data.

One aspect of CFIUS review is the ability for UK firms to provide appropriate protection to the personal data that they hold. The UK data regime surrounding personal data provides stronger protections to individuals than the US federal regime. This means that even when data is managed by the UK there should be limited risk that it would be utilised in a way that could constitute a national security risk for the US. This will continue to be a crucial angle for the UK to emphasise in discussions with US regulators.

The effects of CFIUS review are further exacerbated due to the general lack of transparency in the review process as well as the fact that there is often no burden of proof for when CFIUS decides to block FDI. There is wide scope for CFIUS to act through unilateral action, which operates in a distinctly different way to other more familiar judicial procedures firms may have experienced. Due to this, the review process is viewed as unpredictable and difficult to respond to. Industry would find value in an increase in transparency in both process and final decision. This could be done through increased communication with the firms involved.

The Committee on Foreign Investment in the United States (CFIUS) is an interagency committee chaired by the Secretary of the Treasury which is authorised to review certain transactions involving investment in the US.[3] The purpose of a CFIUS review is to determine the specific investment's effect on US national security.

CFIUS was initially established in 1975 to review and study foreign investment into US businesses. In the late 1980's concern over Japanese investment led to an expansion in the powers of CFIUS through the Exon-Florio Amendment in 1988. This provided CFIUS with the power to directly reject deals due to national security concerns. Since its establishment, CFIUS reviews have covered investments by firms from dozens of countries across the world from OPEC to China. The wide reach and coverage of deals examined illustrates how CFIUS has continued to evolve and adapt to the changing geopolitical landscape.

Traditionally, CFIUS's jurisdictional authority has been limited to reviewing transactions which resulted in foreign "control" of a US business.[4] Control is defined as the power, whether or not exercised to directly or indirectly determine, direct, or decide important matters affecting the US business. In this instance, a CFIUS review would aim to ensure that the proposed change of control would not constitute a national security threat.

Of primary concern to CFIUS is the risk that a change of control would lead to a transfer of funds or technology from an acquired US firm to a sanctioned country or country which poses a national security threat. The belief is that this could occur if the foreign purchaser transfers the knowledge and capabilities of the US firm to another country which would not be possible through the US firm.

Initiating a CFIUS review is a joint voluntary process. CFIUS can, however, independently review any transactions post-closing. Parties to the transaction are, therefore, incentivised to engage based on the risk that the President of the United States might require divestment post-closing if non-mitigated national security concerns associated with the transaction remain.

CFIUS evolution:

Over time, many policymakers became concerned that technological advances had left the original CFIUS framework "insufficient" to address the modern economy's growing complexity and its impact on national security.[5] CFIUS faced growing pressure across 2017 and 2018 including increasing concerns over Chinese investments in US firms and an unprecedented

3 **https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius. https://www.hklaw.com/en/insights/publications/2020/02/new-cfius-regulations-finally-take-effect**

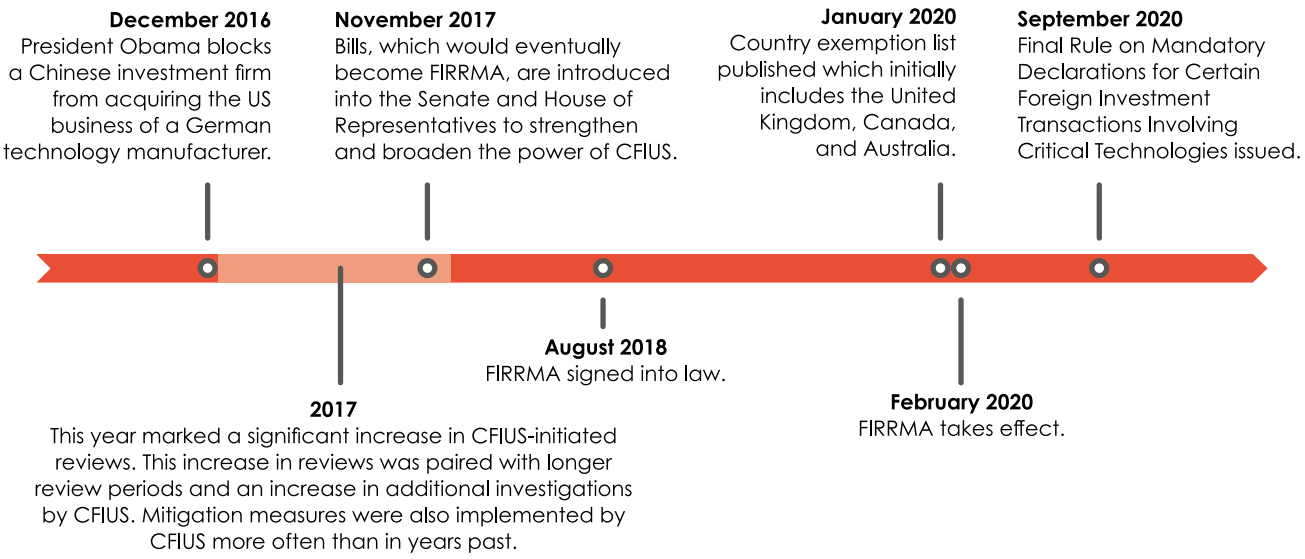
4 31 CFR § 800.204(a).

5 "This bill focuses on providing CFIUS with updated tools to address present and future security needs"- Senator Dianne Feinstein (comment found here). The cosponsors for the reform bill included Republican Senators John Cornyn, of Texas, Marco Rubio of Florida, John Barrasso of Wyoming, James Lankford of Oklahoma and Tim Scott of South Carolina. Democratic Senate co-sponsors included Amy Klobuchar of Minnesota, Gary Peters of Michigan and Joe Manchin of West Virginia. Comment found here **https://www.reuters.com/article/us-usa-regulation-m-a-idUSKBN1D8267**

number of filings over this time period.[6] Such pressures saw bipartisan and bicameral legislative support for CFIUS reform aimed at modernising and expanding the reach these regulations.

The result of these efforts was the passing of The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA). FIRRMA broadens the authority of both CFIUS and the President. It provides them with the ability to review and take regulatory action towards more foreign investment than ever before under the cover of national security concerns. The goal of modernising FIRRMA was to "close the gaps" that had existed between transactions CFIUS was able to review and those transactions that fell outside the regulatory reach of CFIUS yet raised similar national security concerns.[7]

FIRRMA timeline



Scope of FIRRMA changes:

FIRRMA extends CFIUS's reach of review to include minority, non-controlling investment in critical technology, critical infrastructure, and data intensive businesses.[8] In February 2020, regulatory changes through FIRRMA became effective, increasing CFIUS's jurisdiction and outlining changes to its review processes.

6 Several Senators and Representatives have spoken out about their concerns of Chinese investment. This includes Representative Robert Pittenger and Senator John Cornyn who once said during a Council on Foreign Relations event that "[B]y exploiting the gaps in the existing CFIUS review process, potential adversaries, such as China, have been effectively degrading our country's military technological edge by acquiring, and otherwise investing in US companies". (full speech found **here**)

7 US Department of Defense Secretary James Mattis: "FIRRMA would help close related gaps that exist in both the Committee on Foreign Investment in the United States (CFIUS) and export control processes, which are not presently keeping pace with today's rapid technological changes…" (letter to Cornyn found **here**)

8 31 CF Parts 800 and 801

Before FIRRMA, CFIUS-covered transactions were limited to transactions which resulted in foreign control of a US business. FIRRMA extends CFIUS's jurisdiction by expanding the definition of a "covered transaction" so that it now includes:

- A purchase, lease, or concession by or to a foreign person of real estate located in proximity to sensitive government facilities. This also includes real estate that is located within or will function as part of an air or maritime port;
- "Other investments" in certain US businesses (certain critical technologies, critical infrastructure, and sensitive personal data, referred to collectively as TID US businesses) that afford a foreign person access to material non-public technical information in the possession of the US business, membership on the board of directors, or other decision-making rights, other than through voting of shares;
- Any change in a foreign investor's rights resulting in foreign control of a US business or an "other investment" in certain US businesses;
- Any other transaction, transfer, agreement, or arrangement designed or intended to circumvent or evade CFIUS jurisdiction.

This expansion was paired with administrative adjustments to CFIUS through FIRRMA, which include:

- Declarations—Provides for an abbreviated filing or "light filing" process through a new "declarations" procedure that could result in shorter review timelines. It also allows CFIUS some discretion to require parties to file with CFIUS before closing a transaction.
- Expands CFIUS's timelines—CFIUS's review period is extended from 30 to 45 days and allows an investigation to be extended for an additional 15-day period under extraordinary circumstances.
- Mitigation—Strengthens requirements on the use of mitigation agreements, including the addition of compliance plans to inform the use of such agreements.
- Special hiring authority and funding—Grants special hiring authority for CFIUS and establishes a fund for collection of new CFIUS filing fees.

Expansion of mandatory declarations:

The final rule related to mandatory declarations was issued by the US Department of the Treasury in September 2020.[9] This further expanded the scope of which US businesses were required to make declarations and made changes to the definition of "substantial interest". Declarations are now required for certain covered transactions where a foreign government has a "substantial interest" in a foreign person that will acquire a "substantial interest" in a TID US business (i.e., a business involved in critical technologies, critical infrastructure, or sensitive personal data).

9 **https://home.treasury.gov/system/files/206/Fact-Sheet-Final-Rule-Revising-Mandatory-Crit-Tech-Declarations.pdf**

Personal data expansion under FIRMA:

The expansion of a business which handles personal data includes an widening definition of what data this would cover.[10] This includes the following:

- Financial data that might indicate "financial distress or hardship"
- Credit report information
- Insurance application data for health, professional liability, mortgage or life insurance
- Information relating to a person's "physical, mental, or psychological health condition"
- Private emails or other electronic communications
- Geolocation data, including data derived from cell towers, WiFi access points and wearable electronic devices
- Biometric identifiers such as fingerprints and face scans
- Data used for generating government identification
- Data concerning security clearance status
- Data in security clearance application forms
- Genetic test results

Exemptions:

There is an exemption to the expansion of FIRRMA for investors from Canada, Australia, and the UK. These countries were deemed excepted foreign states beginning February 2020 for a period of two years. This status was granted due to the various intelligence sharing arrangements and defence industrial integration these countries have with the US government.[11] This includes those provided under the United Kingdom-United States of America Agreement, also known as the Five Eyes, which enables the default sharing of information between national security agencies.

For each country to remain as an excepted foreign state after this two-year period the state must both be eligible, and the Committee must make a determination concerning the regulatory structure of the state. To do this CFIUS will work to determine whether their national security-based foreign investment review process and bilateral cooperation with the US on these processes meet the requirements of FIRRMA regulations. The assessment is wide ranging and covers everything from the state's legal authority in various circumstances, monitoring and regulatory structures, and national security agreements.[12]

10 **https://www.natlawreview.com/article/spotlight-sensitive-personal-data-foreign-investment-rules-take-force**
11 31 CFR § 800.218; **https://home.treasury.gov/system/files/206/Part-800-Final-Rule-Jan-17-2020.pdf**
12 **https://home.treasury.gov/system/files/206/Excepted-Foreign-State-Factors-for-Determinations.pdf**

To continue receiving an exemption, states must establish a robust process to assess foreign investments for national security risk and facilitate coordination with the US.[13] The review also includes the right for CFIUS to consider other factors which the Committee deems "appropriate" to review in consideration of potential risk. In our interactions with firms, we encountered concerns about the breadth of CFIUS's increased reach. As the review process can include anything that CFIUS deems "appropriate", there are concerns that this could provide an extremely wide range of possible regulations and aspects which could be subjected to the review. Though this is intended to provide CFIUS with flexibility to adapt, it creates uncertainty through its inherent vague wording.

Only in February 2022 will CFIUS add any other countries to this limited initial list.

Exemption limits:

There remain some limits to this exemption. To qualify as an "excepting investor", the individual must:[14]

- Have a substantial connection to an exempted state,
- Not violated certain US laws, including not having submitted material misstatement to CFIUS, violated material provision of a mitigation agreement, been subject to a presidential action under section 721, violated export control laws, or been convicted of a felony in US,
- "Minimum excepted ownership" (at least 50% of a publicly traded company or at least 80% of a privately held fund or entity) must be held by an US persons or citizen of an excepted foreign state who are also not citizens of other countries,
- All directors, observers, and 10% or more owners be from an excepted foreign state

Though investors from these countries are exempt from the new expansion of CFIUS review, they are not exempt from CFIUS' jurisdiction when there is a traditional covered transaction which results in foreign control over a US business.[15]

The impact on UK-based firms:

Private equity firms have avoided most of these changes as their treatment remains in line with prior regulations and current CFIUS practices. There remain four conditions required for US private equity funds with foreign limited partners to not be considered foreign:

- A fund with foreign limited partners must be managed exclusively by a general partner (or equivalent) who is not a foreign person.
- The firm's advisory board which the foreign person sits may not have the ability to control in any way the investment decisions of the firm.

13 **https://home.treasury.gov/system/files/206/Excepted-Foreign-State-Factors-for-Determinations.pdf**

14 31 CFR § 800.219; **https://home.treasury.gov/system/files/206/Part-800-Final-Rule-Jan-17-2020.pdf**

15 **https://www.natlawreview.com/article/expanded-cfius-jurisdiction-affects-foreign-investments-us-certain-countries**

- The foreign person may not have the ability to control the fund, including through investment decisions, ability to approve or disapprove decisions made by the managing partner, or unilaterally determine the compensation of the general partner.
- The foreign person may not have access to material, non-public technical information.

Though these rules seem quite clear, there are several scenarios which could fall foul of CFIUS rules. This includes if a decision requires a unanimous vote by the limited partners which could be construed by CFIUS as a situation where a foreign limited partner has control. Another situation would be if the foreign limited partner has negative voting rights, which CFIUS might believe represents sufficient control by the foreign partner and open the fund open to review. These situations can trigger CFIUS review as they create situations where a foreign individual will have some practical measure of control over the decisions of the US business.

From our discussions it appears that FIRRMA will affect UK firms which are already established within the US more than those which are entering the US market. This is due to the fact that firms expanding into the US have more flexibility in how they structure their US business. Companies just beginning their shift to the US have been able to avoid some of the effects as they are able to begin from scratch and shape the company to fit these requirements. This includes ensuring board members fall into the exemption categories and establishing voting structures which would not trigger a CFIUS review. For established firms, this re-structuring may not be possible or may come at a high cost.

This is not to say that firms expanding into the US are not affected by CFIUS review. Firms often participate in pre-market engagement with US federal departments such as the Commerce Department and Department of Defense. This is paired with due diligence and value chain mapping to highlight that the firm is aware of the source of their investments. The hope is that this work can mitigate the risks from the start. These actions are not without heavy resourcing costs, including sourcing legal advice.

Foundational and emerging technology firms have been disproportionally affected by CFIUS and the expansion of FIRRMA. Due to the expansion of technologies which fall under CFIUS review, many now view potential partnerships with US firms as too risky due to potential blocks by the US government. This will continue to effect firms as technology and strategies expand to cover new ground.[16]

The effects of CFIUS review are further exacerbated due to the general lack of transparency in the review process as well as the fact that there is often no burden of proof for when CFIUS decides to block FDI. There is wide scope for CFIUS to act through unilateral action, which operates in a distinctly

16 An example of this which was provided to us was quantum computing. Though included on the list of technology that is crucial to national security, due to it being an extremely new technology, there is very little knowledge of how it will be utilised in practice. This has led to firms avoiding engaging or experimenting with the technology due to fear of potentially opening themselves up to CFIUS review.

different way to other more familiar judicial procedures firms may have experienced. Due to this, the review process is viewed as unpredictable and difficult to respond to. Industry would find value in an increase in transparency in both process and final decision. This could be done through increased communication with the firms involved.

In 2018, the same year that FIRRMA was passed, the US Treasury released a report into innovation and FinTech in the financial system. This included emphasising the crucial role data plays in lowering costs and breaking down the barriers to entry for new firms.[17] The report states that a wide range of technology-based firms are either competing or partnering with traditional providers in nearly every aspect of the financial services industry.[18] As technology companies continue these partnerships and further engrain themselves into financial services, there is an increased chance of CFIUS review. The expansion of CFIUS's reach to include firms which handle personal data means that FS firms which utilise or partner with tech companies could become subject to review. This increase in oversight and regulation could discourage partnerships between banks and tech companies due to concerns around CFIUS approval. Though the intention behind FIRRMA expansion was to limit foreign intervention and control of data, it may unintentionally create limitations for partnerships between US and foreign firms.

The exemption of the UK for most provisions does provide a reprieve, however this could be strengthened through extended certainty. The two countries are already partners in security through the Five Eyes partnership and already share significant amounts of data between themselves. This should not only limit the national security concerns which CFIUS is meant to manage but illustrates the strong regulatory and governmental ties between the two countries.

Another aspect that will undoubtably be reviewed is the ability for UK firms to provide appropriate protection to their personal data. The UK data regime surrounding personal data also provides stronger protections to individuals than the federal US regime. This means that even when data is managed by the UK there should be limited risk that it would be utilised in a way that could constitute a national security risk for the US. This will continue to be a crucial angle for the UK to emphasise in discussions with US regulators.

Impact of the UK National Security and Investment Bill:

There is a strong possibility that the US could view Chinese investment in the UK as a factor for consideration in a CFIUS review. The perception of Chinese investment in the UK has become a point of increasing concern, both internationally and domestically. In response to increasing the foreign investment in UK, the UK National Security and Investment Bill was introduced to Parliament on 12 November 2020.[19]

17 **https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf**

18 **https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf**

19 Full text of the bill can be found here: **https://www.gov.uk/government/publications/national-security-and-investment-bill-2020**

Background to UK National Security Bill

Up to now, the Competition and Markets Authority (CMA) has been the UK body mainly responsible for investigating national security concerns through a wider process for reviewing "relevant merger situations" that might give rise to public interest considerations. However, concerns have grown about the effectiveness of the current regime in managing the national security risks arising from investment in, or control of, companies and assets in a range of sectors. Technological developments have further widened the potential scope of national security concerns to include such areas as data and intellectual property. The debate over Huawei's role exemplified these concerns.

In 2017, the Government launched a national security infrastructure investment review. This involved an initial consultation on potential future arrangements and resulted in reductions of the thresholds that would trigger a CMA investigation and some widening of the types of economic activity covered (such as inclusion of quantum technology), as well as a wider definition of the types of transaction that would be covered.

A White Paper and a further consultation followed (launched in 2018 with a Government response published on the same day as the Bill). These made clear that the Government wanted a more extensive overhaul of its powers to scrutinise and intervene in investments that raised national security concerns. Rather than leave matters to the CMA, the government proposed to take powers to be directly responsible for national security assessments and be able to intervene in a much broader set of situations that might lead to national security risks.

The Bill therefore sets out 17 sectors of the economy and associated activities that might be encompassed by a mandatory reporting scheme. Some areas include artificial intelligence, communications, critical suppliers to the government and emergency services, and cryptographic authentication services.

Though these do not seem to innately effect FPS, the definitions of these 17 areas remain to be determined and the wide reach of the technology means they could have been

A consultation launched alongside the Bill will run until 6 January 2021, after which the Government has said that it will set out "robust and proportionate" definitions in secondary legislation made under the Bill.

The bill aims to introduce a new regime for reviewing and intervening in business transactions, such as takeovers and investments, that might raise national security concerns. The reach of the bill provides for government review of transactions up to five years after a "trigger event" has taken place. Similar to CFIUS, the UK legislation establishes a requirement for proposed acquirers to obtain approval from the Secretary of State before completion alongside a voluntary notification system to encourage notifications from parties who believe their investment may raise national security concerns.

The question remains on whether this will create a dual regime for UK-US investment where companies from both sides of the Atlantic are required to receive permissions from both US and UK supervisory authorities. Though the introduction of the national Security Bill will most likely be viewed favourably by CFIUS and US regulators in their assessment of the UK's national security regime with regards to the UK's exemption, the biannual exemption renewal process remains unclear. Given the deep connections the UK and US share through G7, NATO, and Five Eyes, the levels of cooperation between the technology sector in the UK and US partners is already incredibly deep. This should provide solid support to any CFIUS FIRRMA exemption provided to the UK and lay the groundwork for any potential extension.

Recommendations:

The effects of CFIUS review are further exacerbated due to the general lack of transparency for firms during the review process as well as the fact that there is often no burden of proof for when CFIUS decides to block FDI. There is wide scope for CFIUS to act through unilateral action, which operates in a distinctly different way to other more familiar judicial procedures firms may have experienced. Due to this, the review process is viewed as unpredictable and difficult to respond to. Industry would find value in an increase in transparency in both process and final decision. This could be done through increased communication with the firms involved.

Though the UK is currently on the exemption country list, it will need to establish a robust process to assess foreign investments to remain so. It is expected that the recently presented UK National Security and Investment Bill will work to ensure this. However, the UK Government should continue to work closely with firms to further develop this regime and seek clarity from US regulators on how to effectively maintain this exemption. This should be paired with advocacy for increased transparency in the review of exemptions by CFIUS.

The Five Eyes partnership and current data sharing arrangements between the US and the UK should not only limit the national security concerns which CFIUS is meant to manage but illustrates the strong regulatory and governmental ties between the two countries. This connection should be emphasised in discussions between UK and US policymakers on extended certainty and increased transparency.

As the UK's personal data privacy regime provides stronger protections to individuals than the US federal regime, there should be limited risk that data held by UK firms would be utilised in a way that could constitute a national security risk for the US. This will continue to be a crucial angle for the UK to emphasise in discussions with US regulators and should provide support to further CFIUS exemptions for the UK.

Data regulation regimes:

Main Takeaways:

The UK and the US share similar goals when it comes to data and digital provisions in Free Trade Agreements (FTAs). There is a chance for the US and UK to build on USMCA to create a gold standard for data and digital provisions in FTAs.

The different and often overlapping data regulation regimes between the US and the UK create barriers for UK firms attempting to access the US market:

- Firms looking to expand to the US or in the early stages of US expansion remain concerned about GDPR and regularly view this as one of the riskiest areas of their business. This is often due to a general lack of in-depth knowledge of the regulations and a lack of resources necessary to provide the granular analysis required. UK firms would benefit from clarity around data privacy regulation, not least as this area of regulation has been further complicated by the recent Schrems II decision's impact on data security and confidentiality. Recent FTC actions, such as the one taken against Zoom, further compound the complex regulatory landscape.
- US regulators remain uncertain of the effects of GDPR on their ability to obtain the necessary data and information to provide appropriate supervision of firms operating within the US. This is illustrated by the SEC Moratorium on Investment Advisor Registration. UK regulators and policymakers should work to provide assurances to their US counterparts that this should not be a concern. This should be achieved through regulatory MoUs and cooperation rather than legislation. Regulatory cooperation per regulated sector, such as through the Financial Regulatory Working Group or other forums for financial services regulators, would be helpful to FPS. Cross-border cooperation between US and UK regulators would give firms greater certainty around compliance with the various regulations of the two countries.
- In the US, there is no single data regulation and protection regime. There exists instead a patchwork of state-level data regulation structures. This lack of US federal regulation in data and the various interactions and differences between state rules regarding data places unnecessary regulatory burden on UK firms. The UK should seek to lobby the US government for overarching structure and guidance for regulation. Federal privacy legislation has been proposed and should be followed to be enacted to provide certainty and uniformity of coverage.

The specific recommendations made for each case illustrate the need for greater regulatory coherence between jurisdictions and, in the case of the US, within the jurisdiction itself.

USMCA data and digital provisions:

Despite this study focusing on the bilateral regulatory relationship, FTAs have a role to play in the data and digital arena.

Earlier this year the US, Mexico and Canada implemented a renegotiated version of the 25-year-old North American Free Trade Agreement (NAFTA), replacing it with the United States-Mexico-Canada Agreement (USMCA). The new digital trade chapter contains many new rules for digital commerce. It prohibits customs duties and other discriminatory measures from being applied to digital products that are distributed electronically.

On data flows, USMCA prohibits the restriction of the cross-border transfer of information if this activity is for the conduct of the business of a covered person. Although there is no specific carve out for financial data within this provision, neither the provisions that prohibit data localisation nor data flow provisions apply to financial services. Instead USMCA provides application of a limited selection of similar measures with regards to financial services within the financial services provisions of the agreement. In USMCA this includes financial services provisions which include a provision for the free flow of data and a prohibition on data localisation.

This is in line with the vast majority of trade agreements which exclude financial services from the reach of data provisions. It remains the ongoing status quo to exclude financial services from the digital and data chapters, with only a handful recent agreements including financial data within provisions on data flows.

The digital chapter of USMCA goes on to limit governments' ability to require the disclosure of computer source code and algorithms. The protection of algorithms is an innovative solution to the issue of the competitiveness of digital suppliers. The USMCA covers not just mass-market software, but all software including critical infrastructure.

In addition, the agreement requires commitment on trade facilitation measures such as the use paperless trading and e-signatures as well encouraging the use of interoperable electronic authentication.

The USMCA has provided the groundwork for future FTA terms on open government data with provisions that commit parties to make government data available to the public in machine-readable and searchable open formats, and allow it to be searched, retrieved, used, reused, and redistributed. This will provide firms with access to government data instead of artificially created data sets and provide them with more accurate insights.

Through the combination of these provisions USMCA represents a high standard in digital trade for the US. The inclusion of clauses on data localisation and the moratorium on digital tariffs and breaking new ground in areas such as cyber security and regulatory cooperation provides a truly wide-reaching digital trade chapter. The UK has the opportunity to utilise this agreement as the starting point both for UK-US discussions and possibly for other agreements.

With UK objectives focused on obtaining a comprehensive suite of FTAs with global trading partners, there is a significant opportunity for the UK and the US to agree digital and data provisions based on shared values. The data transfer and digital elements of the agreement are areas where the sector believes there is potential for advancement between the UK and the US. There is every possibility that the two trading partners may be able to build upon these provisions.

The UK negotiating objectives for an FTA with the US include the facilitation of the free flow of data, whilst ensuring that the UK's high standards of personal data protection are maintained.[20] It is crucial that regulators ensure that the "new Privacy Shield" supports and achieves this free flow of data. They also include provisions to prevent unjustified data localisation requirements and support the reduction or abolition of business and consumer restrictions relating to access to the US digital market.

The UK and the US benefit from having similar objectives in this space and the UK should seek to build upon existing best practice to ensure an inclusion of a robust digital trade chapter in the future UK-US FTA.

USTR Negotiating Objectives
February 2019

- Secure commitments not to impose customs duties on digital products (e.g., software, music, video, e-books).
- Ensure non-discriminatory treatment of digital products transmitted electronically and guarantee that these products will not face government-sanctioned discrimination based on the nationality or territory in which the product is produced.
- Establish state-of-the-art rules to ensure that the UK does not impose measures that restrict cross-border data flows and does not require the use or installation of local computing facilities.
- Establish rules to prevent governments from mandating the disclosure of computer source code or algorithms.
- Establish rules that limit non-IPR civil liability of online platforms for third-party content, subject to the Parties' rights to adopt non-discriminatory measures for legitimate public policy objectives or that are necessary to protect public morals.

UK FTA Objectives
3 March 2020

- Secure cutting-edge provisions which maximise opportunities for digital trade across all sectors of the economy.
- Include provisions that facilitate the free flow of data, whilst ensuring that the UK's high standards of personal data protection are maintained, and include provisions to prevent unjustified data localisation requirements.
- Promote appropriate protections for consumers online and ensure the Government maintains its ability to protect users from emerging online harms.
- Support the reduction or abolition of business and consumer restrictions relating to access to the US digital market.
- Ensure customs duties are not imposed on electronic transmissions.
- Promote a world-leading eco-system for digital trade that supports businesses of all sizes, across the UK.

20 **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/869592/UK_US_FTA_negotiations.pdf**

A recent example of the UK's aspirations with regards to data and digital provisions within an FTA can be seen in the UK-Japan Comprehensive Economic Partnership Agreement (CEPA). Although there is no separate chapter on digital in the CEPA, the provisions included within the Trade is Services chapter are akin to those in the USMCA and CPTPP – deals that have been lauded for the high standard they set in their digital trade requirements.

Of particular note is the CEPA provision for the movement of financial data. This provision is forward looking and is the standard that the UK should be looking to emulate in its trade agreements going forward. Though the provisions on the free flow of data is a definite improvement on the previous EU-Japan Economic Partnership Agreement (EPA), the UK has the opportunity to go further in these areas in any potential US-UK FTA.

On the issue of regulatory cooperation, the CEPA commits the UK and Japan to cooperate and participate in multilateral fora as well as maintain a dialogue on regulatory matters. The UK should seek to go beyond this in subsequent agreements, creating and maintaining channels for regular and sustained cooperation through regulatory means through the establishment of a forum to address issues. The provisions for regulatory and business dialogue outlined in USMCA could provide a solid template.

These provisions, when taken together should help foster the smoother functioning of the digital economy and provide regulatory certainty for businesses. Supporting existing and building new regulatory cooperation mechanisms would be hugely beneficial to UK entities and customers.

Recommendations: The UK should work to further enshrine forward looking digital and data provisions which limit data localisation and ensure the free flow of data, especially in regard to financial services data, within any future FTA with the US.

The UK should work to better understand and learn from the USMCA regulatory dialogues to assess whether, to what extent, and with whom such mechanisms may be most beneficial to replicate in a UK-US FTA.

Data regulation regimes:

The fragmentation of regulation between the US and the EU/UK system creates barriers for UK based FS firms attempting to access the US market. Issues such as the differences between data protection regimes, changes in regulation, and general lack of direct comparison between regimes is problematic. There are specific recommendations that can be made for cases where barriers exist. These, however, all feed into the overarching goal of greater regulatory coherence, whether that be within a certain jurisdiction, between jurisdictions, or on a global level.

GDPR and Schrems II:

For FinTech and other firms expanding into the UK, GDPR remains a major issue when it comes to their day to day functioning. Many remain extremely cautious in this area for fear of unintentionally falling foul of GDPR regulations. This has led to UK firms expanding into the US working to avoid potential conflicts through localisation of data and even email addresses to US servers to avoid GDPR and Privacy Shield issues.

This creation of silos for data from various jurisdictions is often due to the fact that data is one of the areas of least knowledge for these firms. For start-ups and digital-first firms even developing the knowledge to navigate these regulations can be an onerous task. This means that they often take the path of least resistance in the immediate timeframe by localising data to avoid potential cross-country data flow regulation concerns. Although this solves the problem in the short-term, it creates a large administrative burden on firms to establish and manage these structures and may lead to bigger problems in the long run.

The recent Schrems II decision now also means that firms themselves have a responsibility to assess the level of data protection in the jurisdiction where they are sending data. Conversations with firms have highlighted that this uncertainty could create the perverse potential incentive of localising data to avoid the ambiguity surrounding GDPR regulations.

Schrems II summary

The UK, as part of the EU, has benefited from Privacy Shield and its predecessor the Safe Harbor Agreement. Both agreements supported free data flows between the US Privacy Shield signatory companies (which did not include financial services, telco's and other regulated firms in the US) and various EU countries by providing legal opinions on such transfers. Through Privacy Shield, the EU Commission held that US regulatory and governmental assurances concerning intelligence mechanisms and legal protections offered adequate protection for EU personal data. Most companies entered into Standard Contractual Clauses (SCCs) to provide further protection for the personal data it transferred to the US and with those US firms for whom Privacy Shield was not available.[21]

SCCs are also subjected to EU supervisory authorities, who can suspend or prohibit data transfers if it concludes that law of the country to which the personal data is transferred to cannot comply with the obligations set out in the SCCs.

The Schrems II case disputed whether these assurances and SCCs were enough to provide the data privacy outlined in GDPR. On 16 July 2020 the Court of Justice of the European Union (CJEU) ruled that the protection provided by the EU-US Privacy Shield is not adequate and it is therefore no longer an adequate mechanism for the transfer of personal data from the European Economic Area (EEA) to the US. The CJEU continues to have fundamental concerns with US surveillance law and the right to legal action against US authorities for EU citizens. Furthermore, the ruling stated that the US oversight mechanisms did not have binding authority over the US national security institutions.

Despite this, the CJEU ruled that SCCs remain valid. However, this was provided with the caveat that SCCs on their own may not be enough to ensure an adequate level of protection. To certify SCCs provide an appropriate level of protection for personal data, firms must prove that data can only be transferred if firms transferring and receiving the data are able to ensure that SCC protection can be complied with in practice. The judgment implies that supervisory authorities have a role in assessing whether the data is subject to an adequate level of protection. Guidance on how to carry out such an assessment remains high-level for the time being with the only guidance being that the parties can consider supplementary measures to ensure an "equivalent level of protection" of personal data as provided in the EEA.

Further detailed guidance as to what these supplemental measures might look like has been recently adopted by the European Data Protection Board (EDPB).[22] The EDPB acknowledged that SCCs "do not operate in a vacuum" and hence are required to be accompanied by other stringent actions by firms to ensure that their data transfer is compliant following Schrems II. Following their adoption, the EDPB has released the recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, providing a step-by-step action plan for international data transfers:

1. Know the transfers;
2. Verify and choose a transfer tool;
3. Assess recipient country's laws;
4. Apply supplementary measures to the EU standard of essential equivalence;
5. Take any formal procedural steps to make sure these work;
6. Repeat and re-evaluate.

The EDPB welcomed comments on the recommendations until the end of November 2020.

continues...

21 Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46 (OJ2010 L39, p.5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L344, p.100).

22 Full EDPB guidance can be found here: **https://edpb.europa.eu/news/news_en**

These provide data exporters with the standards required to meet GDPR obligations through SCCs and therefore transfer data outside the EU. However, the current status remains one of great uncertainty as to whether, even if more detail is provided, exporting companies will be able to meet their new standards. The recommendations on supplementary measures continue to be consulted on, but are very onerous, particularly for SME's. As each individual data transfer will need to be assessed on a case by case basis, smaller firms will be forced to devote an increased amount of resources to ensure continued compliance.

It is crucial that regulators ensure that the "new Privacy Shield" and measures surrounding its implementation supports and achieves the goal of the transatlantic free flow of data.

Lack of local comparison in data regulation:

There can also be a general lack of understanding between US and UK regulators on policy which has no local comparison (i.e. GDPR v US data protection regulations at the Federal level, or lack thereof). This can cause misalignment and unintentional policy barriers between the two. This was recently seen in the asset management industry through the SEC moratorium on the registration of EU and UK firms (see below) and is seen by FinTechs deliberately storing data in the US to avoid potential GDPR infringements.

Case Study: SEC Moratorium on Investment Advisor Registration (GDPR)

Relevant legislation: Perceived conflict between the US Advisors Act of 1940 and GDPR

The SEC requires investment managers to complete forms ADV part 1 and 2 to register in the US as investment advisors (RIAs). The forms request information about the firm, its services, fees and disciplinary disclosures, and employment and conflict of interest information. These forms are an prerequisite to gaining the SEC's Investment Advisor Registration.

From 2018 to 2020, the SEC stopped approving applications and placed a block on the registration of EU and UK-based investment managers under the US Investment Advisers Act of 1940. This was due to stated concerns held by SEC staff over the impact of GDPR on firms' ability to transfer personal data to the SEC and respond to information requests for the purposes of examination.[23]

In order for an application to be considered by the SEC, investment managers were asked to provide a legal opinion from US counsel as to their ability to provide personal data to the SEC. This included confirmation that the applicant could provide the SEC with prompt and direct access to its books and records, as a matter of law and practical application. Due to the requirements set out under GDPR, most lawyers were unable to provide confirmation of practical application without including some qualifications for the data transfer. Although some opinions had been provided by firms, the registration filings remained unprocessed due to the moratorium.

23 **https://www.ft.com/content/37fcad82-159b-11e9-a581-4ff78404524e**

This created a barrier as even once a legal opinion was obtained there was no guarantee that the application will be processed. This requirement to provide it created an administrative burden that was unaffordable to smaller firms. The added uncertainty around even obtaining SEC approval meant that some firms decided not to attempt to gain registration.

With the US standing as the world's largest asset management centre, with $21.17 trillion in total assets managed, and the world's largest mutual fund industry, it is the premier choice of domicile for the hedge funds and private equity funds industry. For the UK-based investment management industry, access to the US markets is key to maintaining its role and reputation as a global hub for investment management. Given this, the block on SEC registrations acted as a great barrier to investment.

UK investment managers were compelled to forgo investment advisory mandates ranging from hundreds of millions to billions of US dollars and cease offering and distributing their products in the US. Firms also faced additional compliance costs, costs that disproportionally affected smaller firms. In addition to impacting the large pipeline of firms seeking to register with the SEC, the block on SEC registrations placed already registered UK RIAs at risk of being suspended or de-registered in annual re-certifications. Over 60 UK investment managers had been formally denied registration and an undefinable number of firms chose not to pursue registration, due to the administrative costs involved and lack of likely approval. The moratorium also impacted US investors – of the 12,600 SEC investment advisers, the UK makes up 31% and manages $4,835 trillion in assets under management.

One possible solution offered was for the SEC to enter into Model Contractual Clauses. Model Clauses act as a contract between two legal entities and do not require a license. This contract is a standardised format provided by the EU and provides for a standardised methodology for transferring personal data to controllers and processors located outside the EEA. There remain issues with utilising Model Clauses as they do not fit to all circumstances. Large firms which operate through a branch structure may require hundreds of clauses to cover the various entities which engage with the data handled by the firm. This can be administratively difficult and will often be quite expensive. Though this is a readily available option which could be utilised by firms, albeit possibly with some difficulty, the SEC has stated they will not engage in Model Clauses in regard to their concerns surrounding GDPR. It is worth noting that the SEC is not alone in this as no regulator has agreed to embrace model clauses as a solution to GDPR concerns.

This means that any solution to data transfer between the UK and US was forced to rely on Article 49 GDPR on Derogations for Specific Situations. Article 49 of GDPR outlines when data can be transferred to a third country in the absence of an adequacy decision.[24] Article 49 of the GDPR is generally viewed as unhelpful to firms and the penalties firms face for breaches have left firms more risk averse when it comes to GDPR compliance.

24 **https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf**

Another solution presented was for a firm to form a US subsidiary or go through a US-based affiliate when seeking SEC registration. This is an option only available to larger firms, however, which left smaller firms in limbo. The moratorium therefore disproportionally effected smaller firms who are faced with increased administrative costs in order to register and are unable to utilise US-based outfits.

After more than two years of working to lift the moratorium, the Alternative Investment Management Association, Investment Association and several industry representatives and Government departments successfully facilitated a solution.

The bodies encouraged the UK's Information Commissioner's Office (ICO), the UK's data regulator, to submit an opinion to the SEC clarifying that firms could, and can, rely upon certain legal bases under GDPR to transfer relevant personal data.[25] The written opinion provided to the SEC outlined GDPR requirements for UK firms and the assurance that data from UK firms would be provided to the SEC in case of potential examinations.

The Opinion was accepted by the SEC and, in September 2020, it publicly confirmed that it would begin registering UK firms. As the SEC applied the moratorium to all EU Member States, the ICO's resolution, the first across all impacted EU jurisdictions, was welcomed by the UK investment management industry and provided a competitive advantage to UK firms.

The issue faced by UK investment managers provides an insight into the potential impact of fragmentation and lack of local comparison in data privacy laws. Asset management firms frequently cited that the framework for cross-border transfers of personal data under GDPR does not appear to have changed materially from the superseded Data Protection Directive 95/46/EC. It remains unclear what caused the SEC's shift in policy, though the greater global scrutiny into data protection, as propelled by GDPR, could have prompted the SEC to take a more cautious approach to handling EU and UK data. Uncertainty surrounding the Safe Harbor regime which continued with EU-US Privacy Shield, despite it being designed to be a solution, could also have contributed to the SEC's increased precautions.

Nonetheless, the two-year moratorium highlights how miscommunication between policymakers can lead to outsized effects on an industry. In this case, an absence of local comparison and communication between policymakers and regulators restricted the ability for UK regulated entities to share personal data with a US regulator, disrupting legitimate financial supervisory activities.

This outlines the crucial role communication between policymakers and regulators provides. Clear communication on the change, or lack thereof, in relevant provisions from the Data Protection Act 1998 to GDPR in areas such as regulatory access to data would provide beneficial insight and assurance to non-EU regulators.

25 The role of the UK Information Commissioners Office (ICO) is to uphold information rights in the public interest, promoting openness by public bodies, and data privacy for individuals. This includes UK implementation and enforcement of GDPR.

International regulatory dialogue:

Internationally, information sharing between regulators is crucial, yet the differences in data regulation regimes can create problems when it comes to the practical application of this goal. This can be further complicated by a countries' assessments of other regimes.

The UK and the US should work together to not only achieve bilateral solutions but support international work towards global solutions through international organisations such as the OECD, WTO, and G20/G7. The open communication between the UK and US government can provide a strong groundwork for discussions and collaboration on a larger scale to support finding common ground and solutions.

The OECD principles and convention 108 bases equivalence on an assessment of the outcomes-based core principles of the regulation. This could be utilised to provide the foundations for regulators to establish their own assessments of foreign regulatory regimes.

By focusing on shared outcome goals, national regulators can provide other countries with equivalence even if the processes are different. This could encourage regulatory cooperation between countries which share similar outcomes focused regulations. The hope is that these assessments could provide for the free flow of data through acceptance of laws based in similar principles without requiring identical laws.

Recommendations: Broader regulatory cooperation between the US and the UK should work to be forward facing and enable discussions of potential future regulatory issues which could create unintentional barriers to market access. By understanding the responsible regulators on both sides of the Atlantic and ensuring appropriate dialogue between them, this can be avoided. Through establishing appropriate regulatory dialogues, both sides can better understand the regulatory reach, aims, and concerns of their counterparts.

By understanding the responsible regulators on both sides of the Atlantic and ensuring appropriate dialogue between them, this can be avoided. Further building on pre-existing regulatory cooperation would be hugely beneficial to UK entities and customers. Through establishing appropriate regulatory dialogues, both sides can better understand the regulatory reach, aims, and concerns of their counterparts.

State vs federal data regulation regimes:

Fragmentation is not only an issue faced on the global level, it can also exist within a jurisdiction. This is the case for data privacy regulation in the US.

In the US, there is no single data regulation and protection regime. There exists instead a patchwork of state-level (eg. CCPA) and sector specific (eg HiPPA, GLBA, COPPA etc) data regulation structures. This lack of US federal regulation in data and the various interactions and differences between state rules regarding data in the US further exacerbates the situation for UK firms engaging in the US market.

As UK firms are bound by GDPR, the complex collection of US regulations and obligations can quickly become unwieldly. The lack of a single federal US framework around data privacy creates difficulty in providing an overarching assessment of data protection. Under GDPR, a UK firm would be required to provide an assessment of data regulations for each state and each sector in which they operate. This means if a firm operates across the entirety of the US it would need to complete 50 separate assessments to meet GDPR requirements according to EU regulation and for each relevant sector.

Currently the only US states with data privacy laws are California, Nevada[26], and Maine[27]. Each separate state regulation places data privacy responsibilities on different firms, from internet providers to any firm which handles data. For UK firms engaging in the US, the California Consumer Privacy Act (CCPA), recently expanded and strengthened by the California Privacy Rights Act (CPRA), remains the most comprehensive US standard for managing data in the US. Though this regulation only applies to California, the lack of any federal regulation in this space has led to a heavy reliance on compliance with CPRA. A federal data regulation would be beneficial, but at the time being there are so few states with data protection legislation and regulation that it is not an issue. The larger tech companies (Microsoft/Google/Apple) continue to lobby the federal government for a single overarching national data regulation. As these international firms are often already working to meet GDPR requirements, their requests are often for the US to develop something similar. Though Fintech often lack the same lobbying power and resources to push for this themselves, they do provide their support.

26 Nevada: Senate Bill 220 "An Act relating to Internet Privacy", found on the Nevada Electronic Legislative Information System, **https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6365/Overview**

27 Act to Protect the Privacy of Online Customer Information **https://www.maine.gov/governor/mills/news/governor-mills-signs-internet-privacy-legislation-2019-06-06**; **https://www.mainelegislature.org/legis/bills/bills_129th/billtexts/SP027501.asp**

What is CCPA and CPRA?

The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them. This landmark law secures new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.

Businesses are required to give consumers certain notices explaining their privacy practices. The CCPA applies to many businesses, including data brokers.

Source: State of California Department of Justice

In November 2020, the CCPA was expanded and strengthened by the California Privacy Rights Act (CPRA). The CPRA strengthens the CCPA through establishing a new government agency responsible for handling the enforcement and compliance with CCPA and any new privacy regulations. This was paired with an expansion of the reach of the CCPA. One of the largest impacts of this change in regulation is that firms are now responsible for what happens to the data they collect on California residents. If a firm shares the data they have collected to another firm, the firm which originally collected the data from California residents will be held responsible for any infringement on the personal data rights of those individuals. The CPRA also provides for the right of any California resident to update their personal information and requires firms to allow for consumers to do so.

CCPA with CPRA expansion vs GDPR: a comparison

Similarities:

- Definition of central terminology.
- The right for the individual to access their personal information.
- Both CCPA and GDPR establish additional protections for individuals under 16yr old and their personal information and data.
- In both CCPA under the CPRA expansion and GDPR, firms are responsible for not only compliance with their own collection of data, but also for what happens to that data if it is passed on to another firm

Differences:

- The main difference between CCPA and GDPR are in the way which personal data rights are provided to firms. GDPR requires firms to be even express rights by the individual to their data (opt-in) while CCPA requires the individual to opt-out of providing the firm with access to their data.
- The fundamental principle of GDPR is the requirement for firms to have a legal basis for processing of personal data. This reflects how the EU places ownership of the information with the individual whereas CCPA places ownership of the data with the company.

Other differences include:

- Scope of application and data covered
- Nature and extent of collection limitations
- Rules governing accountability
- Transparency obligations
- Rules regarding data transfers in the case of mergers and acquisitions

Further examples of fragmentation within US regulation is the requirement firms face regarding data breach notifications. These regulations place a requirement that individuals be alerted when their data is exposed in security incidents.[28] Although all 50 states have enacted data breach notification statutes, there is a wide variety of regulations. This includes differences in various term definitions, what data is covered, what entities are required to provide notifications, time limits to provide the notifications, and how to notify the consumer among other things.

This means that to issue the data breach notification firms must complete a separate notification for each state in which they operate. The lack of federal guidance in this area creates a high administrative burden on firms who operate across multiple states. Though notifications are only issued when a data breach occurs, the different regulations for each state could lead to firms unintentionally falling foul of regulations and unintentional mistakes. Though firms could set the standard at the highest requirements among the states in which they operate, it would still require each notification to be filed appropriately with the various states.

28 **https://iapp.org/media/pdf/resource_center/Data_Breach_Notification_United_States_Territories.pdf**

Federal guidance or coordination through state level regulatory cooperation could lessen the burden on firms caused by the innately fragmented structure of US state level regulation. State regulators already have various coordination groups in other areas, such as the Conference of State Bank Supervisors (CSBS). Increased dialogue and cooperation mechanisms between state level data regulators could supported increased coherence at the state level, along with knowledge sharing. UK policymakers should work to support such efforts to increase interaction between federal and state level regulators and their UK counterparts.

Recommendation: Regulatory cooperation per regulated sector which provides the basis for meaningful exchange between the UK and the US for financial services would help provide greater certainty around compliance with the various state regulations and be welcomed by UK regulated organisations.

The UK should work to encourage the US to embrace Federal privacy legislation rather than state by state, as with breach notifications, which often leads to fragmentation and significant administration and legal burdens for firms. Not only would a federal privacy regime decrease fragmentation but could also address the barriers created through the EDPB Schrems II guidance for the UK and EU to share data with the US. The recent US Congressional hearings reflect an increasing appreciation across the US Federal Government of the impact, both positive and negative, of tech for US citizens and beyond.[29]

29 **https://www.reuters.com/article/usa-tech-senate-idUSKBN27D1BQ**

Conclusion

This report should be viewed as the first in a series of reports analysing the current and future of the UK-US FS relationship. Through analysing the potential market access barriers faced by UK firms when operating, expanding, or considering engaging in the US market, the reports will highlight key areas for greater regulatory cooperation. They will also cast a light on areas where further analysis on existing mechanisms and processes which could be utilised to the mutual benefit of the UK and US.

Our discussions with UK firms highlighted the importance of the US market for UK firms, be that in terms of profitability, its forward looking regulatory regime or cultural similarities. The further strengthening of this relationship is a key priority for the UK evidenced by the prioritisation of the US in trade negotiations.

The significant challenges faced by economies in dealing with the global Covid-19 pandemic and the subsequent recovery provides further impetus to liberalise market access between key trading partners - an area where the UK and US can build on their leadership to ensure the continuation of trade and ultimately drive prosperity.

The City of London Corporation would like to thank those who assisted us in our research and contributed to this report. They have provided invaluable and detailed insights into how UK firms operate in the US and what the future UK-US relationship could look like. We welcome further comment on the issues presented in this report and others facing UK firms engaging in the US market.

Acknowledgements

The City of London Corporation would like to thank everyone who has given their time during the production of this piece of work and contributed to this report. They have provided invaluable and detailed insights into how UK firms operate in the US and what the future UK-US relationship could look like. We will include a full list of contributors and acknowledgements in the final report in this series.

Contributors to the Report

Alexandra Mills
Senior Global Trade Policy Adviser

+44 (0) 7544 656861 | alexandra.mills@cityoflondon.gov.uk

Duncan Richardson
Head of Global Trade Policy

+44 (0) 7841 514872 | duncan.richardson@cityoflondon.gov.uk

Tehreem Yusuf
Global Trade Policy Adviser

+44 (0) 7841 533719 | tehreem.yusuf@cityoflondon.gov.uk

The UK-US Regulatory Relationship

A study into the UK-US regulatory market access barriers

Foreign Investment Screening and Data Privacy Regulation