UPDATES ON CHINA TRADE: NAVIGATING A COMPLEX AND CHANGING LANDSCAPE

June 6, 2019

Giovanna M. Cinelli
Practice Lead, International Trade &
National Security
Morgan, Lewis & Bockius LLP

Where are we today?

- US-China relationships stand at a crossroads today across sectors:
  - Trade
  - Cybersecurity
  - Supply chain integrity
  - National defense
  - Global integration of research and development
  - Emerging technologies
  - Finance

Managing the Landscape

- US-China government interactions have risen to a new level of inconsistency reflected in
  - Policy announcements
  - New legislation
  - Executive actions reflected through Executive Orders, policy directives, guidelines, and the exercise of existing legislative trade authorities under longstanding statutes – e.g., Sections 232, 201, 301, and US export laws
  - Multi-government engagements

Managing the Landscape

- Managing the landscape benefits from understanding where, when and how changes to policies immediately impact business decisions
  - Some areas – such as trade requirements – build in ‘wind down’ or ‘ramp up’ periods that allow businesses to shift gears in a more measured way
  - Other areas – such as supply chain and sanctions – take effect when issued or include narrower ‘wind down’ periods
  - The US-China relationship presents both consistent and unique challenges given the integrated nature of the countries’ engagement – e.g., supply chain, research and development, academic studies, and dual use technology development
  - The relationship is further complicated by the insertion of international oversight and standards such as the World Trade Organization and GATT

Areas to Consider

- The geopolitical circumstances and the ongoing policy shifts makes it more challenging to plan for or preempt disruptions to business overall
- These disruptions are most keenly felt in areas where longstanding interrelationships exist that cannot be undone or transformed absent impactful changes that create upstream and downstream consequences
- The inability to plan for or preempt such disruptions undercuts the certainty that businesses seek when handling complex global transactions or engaging in development activities that focus on multi-country and multi-organization participation
- Although these types of disruptions are not new – i.e., changes in export laws have consistently been cited as disruptive to global business – the frequency of these disruptions and the nature in which the disruptions are created inject additional uncertainty, expense and delay

Where Disruptions Occur

- Several key disruptive factors merit attention given the current relationship between the United States and China
  - Addressing the Supply Chain (which is integrated with cybersecurity, based on the 'information grid matrix' that applies to procurements and parties in the procurement chain)
    - Who, what, where, when and how?
    - Understanding the problems to find the solutions
  - US Export Controls
    - What does the Export Control Reform Act of 2019 signal for dual use products and technology?
    - What role do sanctions play?
  - Cybersecurity
    - What standards exist that may interrupt the flow of data – whether technical, personal, financial, or business related?
  - Foreign Direct Investment
    - In the United States by Chinese parties
    - In China by US parties

Supply Chain and Cybersecurity
Identifying the Problem

- "The U.S. is under systemic assault by foreign intelligence entities (FIEs) who target the equipment, systems, and information used every day by government, business, and individual concerns." Supply Chain Risk Management Background Paper (National Counterintelligence and Security Center, Supply Chain Directorate)(2018)

- "A major factor enabling supply chain threats has been the globalization of our supply chains, characterized by a complex web of contracts and subcontracts for component parts, services and manufacturing extending across the country and around the world. The multiple layers and networks of suppliers in this chain are frequently not well understood by either manufacturers or consumers. Our most capable adversaries can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversions." Supply Chain Risk Management Background Paper (National Counterintelligence and Security Center, Supply Chain Directorate)(2018)

- A supply chain is only as strong as its weakest link. The cyber threat from foreign adversaries, hackers, and criminals presents significant and new risks to government and industry. Constant, targeted, and well-funded attacks by malicious actors threaten government and industry alike by the way of their contractors, sub-contractors, and suppliers at all tiers of the supply chain. Sophisticated threat actors exploit vulnerabilities deep in supply chains as a beachhead from which they can gain access to sensitive and proprietary information further along the chain. Supply Chain Risk Management, Cybersecurity and Infrastructure Security Agency, DHS (2019)

- "[F]oreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people." Executive Order on Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019

Supply Chain Cybersecurity
Why Does It Matter?

- "America's manufacturing and defense industrial base consists of the end-to-end set of capabilities, both private and public, that design, produce, and maintain platforms and systems (hardware and software)…. With ***an extensive, multi-tiered global supply chain,*** the industrial base encompasses the extraction and refinement of primary materials, the manufacturing of components and parts, and the ***integration and sustainment*** of … platforms and systems. It relies on a ***geographically and economically diverse network*** of private sector companies, R&D organizations, academic institutions, and government-owned facilities to develop and produce …technologies…." (Emphasis added)
  - (Report to President Donald J. Trump by Interagency Task Force in Fulfillment of Executive Order 13806: *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (September 2018)
- "Federal agencies ***and other entities*** need to take urgent actions to implement a comprehensive cybersecurity strategy, perform effective oversight, secure federal systems, and protect cyber critical infrastructure, privacy, and sensitive data." GAO-19-157SP. *High Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas ("Ensuring the Cybersecurity of the Nation")(March 2019), at p. 178*
- The Government Accountability Office first designated cybersecurity as a risk in 1997
  - Identified the protection of critical infrastructure assets in 2003
  - Identified the protection of personal identifier information in 2015
- These issues affect a range of parties and benefit from a coordinated approach (Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806: *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States (September 2018), p. 9*

Supply Chain Cybersecurity
Why Does It Matter?

- Executive Order 13806 outlined areas of concern such as:
  - The erosion of the US industrial base
  - The threat (both long and short term) to the US lead in existing and emerging technologies
  - The persistent press by multiple adversaries of cyber intrusions; and
  - The critical loss of intellectual property
- These concerns inform how we define the cybersecurity threats independent of and in conjunction with the supply chain
- The US has developed an overarching approach to cybersecurity and supply chain requirements through laws, regulations, policies and directives, designed to identify the threats, determine the vulnerabilities, assess the consequences, and ultimately, manage risk

Defining Cybersecurity and Supply Chain

- Cybersecurity and supply chain – as concepts – are generally understood to include:
  - Cybersecurity: "Definition: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation
  - Extended Definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the information and communications infrastructure."

    CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009
  - Supply Chain: "Definition: A system of organizations, people, activities, information and resources, for creating and moving products including product components and/or services from suppliers through to their customers

    Related Term(s): supply chain risk management. CNSSI 4009, NIST SP 800-53 Rev 4"
  - Supply Chain Risk Management: "Definition: The process of identifying, analyzing, and assessing supply chain risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

    DHS Risk Lexicon, CNSSD 505"

Defining Cybersecurity and Supply Chain

- Unique aspects of cybersecurity and supply chain:
  - The interrelationship (or symbiotic relationship) between governments and organizations
  - The difficulty in identifying and/or remediating issues
- Threats include, but are not limited to:
  - External actors
  - Internal actors
  - Comprised systems
  - Comprised services
  - Unidentified risks (lack of knowledge of the threat)

Defining Cybersecurity and Supply Chain

- Vulnerabilities include, but are not limited to:
  - Weak security protocols
  - Poorly trained work force
  - Lack of ‘cyber hygiene’
  - Unenforced company policies
  - Improperly implemented regulatory requirements – *i.e.*, failure to obtain export authorizations for transfers
- Consequences include, but are not limited to:
  - Loss of data (destruction)
  - Data corruption (segments of data are unreliable)
  - Data manipulation (reorienting or restructuring data, such as reconfiguring a bill of material)
  - Data exfiltration (theft)
  - System disruption (denial of service or denial of access)
  - System compromise or manipulation (known or unknown)

Cybersecurity and Supply Chain Legal, Regulatory and Policy Requirements

- Legal landscape and current issues
  - EO 13873 of May 15, 2019: Executive Order on Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689-22692 (May 17, 2019)
  - Federal Information System Management Act of 2014 (FISMA), 44 USC 3551, et seq. (PL 113-283)
  - National Defense Authorization Act of FY 2011, Supply Chain, 10 USC 2339a
  - National Defense Authorization Act of FY 2019, PL 115-91 (§ 881 updates supply chain requirements)
  - National Defense Authorization Act of FY 2019, PL 115-91 (include §§ 845, 871, 885, 113, 1639, 1645, 1648, 1650 and 1654)
  - "Requirements related to Supply Chain Risk," 80 FR 67244-67252 (October 30, 2015), updated 84 FR 4368-4370 (February 15, 2019); DFARS 252.239-7018 and DFARS 252.239-7017
  - "Restrictions on Acquisition from Foreign Sources," 83 FR 65560-65562 (December 21, 2018)
  - PDD 21: Critical Infrastructure Security and Resilience Directive (identifies 16 key sectors)
  - PDD 21: Critical Infrastructure Security and Resilience Profram (C-SCRM) (DHS and NIST)
  - DHS Binding Operational Directives (e.g., 'do not buy' lists or 'remove from systems' lists)
  - US Homeland Security, Defense and General Acquisition Regulations and Directives

What Issues Exist?

- Managing supply chain risks created by compliance obligations
  - Modifying contract language concerning the definition of compliance
  - Establishing contract requirements that assign responsibilities for various legal obligations – e.g., Who is required to certify regarding the reliability or quality of a product? What mandatory flowdown provisions (whether from government or commercial contracts) apply?
  - Establishing conflict of law “avoidance” processes – e.g., Clauses that identify more specifically which laws prevail under what circumstances
  - Establishing time limits to accommodate changing geopolitical and legal circumstances – e.g., Rather than open ended contracts that continue unless terminated, consider clauses that set time periods for contract performance and require affirmative confirmation for the contract to remain effective

Export Controls

- US Export Controls
  - US export controls have been longstanding tools of US foreign policy and national security since the early 1800s
  - Understanding where export controls have been and where they are today is essential to assess where they may move in the future
  - This understanding requires a candid assessment of the manner in which the controls apply and their effectiveness
  - Application and effectiveness may be determined by the manner in which the US licenses products and technology and the level of enforcement for breaches of the laws and regulations
  - Two basic philosophies underpin US export controls:
    - Deny access or delay access to products and technology to maintain an advantage – whether national security, foreign policy or competitive
    - “Run faster” than competitors or adversaries so that you may share products and technology more freely

Export Controls
Why Do They Matter?

- Export controls and licensing "broaden[] the U.S. Government's visibility into transactions involving national security controlled items on the Commerce Control List and exports, reexport and transfers (in-country) to and in a country of concern." 84 Fed. Reg. 24081-24021 (May 24, 2019)
- To the extent that trade secret and export controlled information overlap: "From 2011-2018, more than 90 percent of the Department [of Justice's] cases alleging economic espionage by or to benefit a state involve China and more than two-thirds of the Department's theft of trade secret cases have had a nexus to China." Statement of John C. Demers, Assistant Attorney General, Department of Justice before the Committee on the Judiciary, US Senate for the Hearing on "China's Non-Traditional Espionage against the United States: The Threat and Potential Policy Responses" (December 12, 2018)

Export Controls
Why Do They Matter?

- "Civil-Military Fusion"
- Made-in-China 2025 policies
- 5 and 13 year plans regarding civil-military fusion and technology areas of interest for the development of indigenous capabilities
- "Forced technology transfers" which require export authorizations from the US Government
  - US Commercial Technology Transfers to the People's Republic of China (Bureau of Export Administration, Office of Strategic Industries and Economic Security, Defense Market Research, Department of Commerce)(January 1999)
    - Reflects a longstanding area of concern
    - Is focused on 'dual use' and 'civil-defense industrial policies' of China
  - USTR Report on China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property and Innovation (Reports from March and November 2018)

Export Laws and Regulations

- Two primary regimes govern the majority of exports from the United States
  - Export Control Reform Act of 2018, PL 115-232 (as included in the National Defense Authorization Act of 2019) (follow-on to the Export Administration Act and the Executive Orders issued under the International Emergency Economic Powers Act)
  - Arms Export Control Act, 22 USC 2778 *et seq.*

Export Laws and Regulations

- Export Control Reform Act of 2018 (“ECRA”)
  - Administered by the Department of Commerce, Bureau of Industry and Security
  - Implemented through the current Export Administration Regulations, 15 CFR parts 730-774
  - Focuses on dual use products, materials, equipment, software and technology (collectively, “items”)
  - Establishes a licensing, recordkeeping and reporting framework based on national security and foreign policy considerations
  - Treats countries differently – i.e., the EAR provides different standards for licensing items to various countries
  - Requires licenses or the use of license exceptions
  - Maintains a detailed list (the Commerce Control List) of items that are subject to control

Export Laws and Regulations

- Export Control Reform Act of 2018 ("ECRA")
  - Include provisions which tie export controls to foreign direct investment
  - Section 1758 of ECRA
    - "Emerging technologies"
    - "Foundational technologies"
  - Recent developments
    - 83 Fed. Reg. 58201-58202 (November 19, 2018) – "Review of Controls for Certain Emerging Technologies"
    - 84 Fed. Reg. 23886-23899 (May 23, 2019) – "Implementation of Certain Controls on Emerging Technologies Agreed at Wassenaar Arrangement 2018 Plenary"

Export Laws and Regulations

- Recent actions
  - EO 13873 of May 15, 2019: Executive Order on Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689-22692 (May 17, 2019)
    - Provides broad discretion to affect activities with “foreign adversaries”
    - Is designed to affect “transactions” which pose undue risks of sabotage or subversion to information and communications technology or services OR which pose an undue risk of catastrophic effects on the security or resiliency of US critical infrastructure or the digital economy
    - Requires regulations within 150 days from May 15, 2019 (expected to be published by October 13, 2019)
    - Delegated to the Department of Commerce – which overlaps with Commerce’s responsibilities for emerging and foundational technologies (under foreign direct investment requirements) and enforcement authorities under the EAR

Export Laws and Regulations

- Recent Actions
  - 84 Fed. Reg. 22961-22968 (May 21, 2019)(but effective May 16, 2019) – “Addition of Entities to the Entity List”
  - Enforcement type action on the part of Commerce
  - Designed to limit interactions between specific parties and US entities – in this case: restricted exports, reexports and transfers of items “subject to the EAR” to Entity List designated parties
  - All license requests are viewed under a presumption of denial standard
  - No license exceptions apply
  - Commerce softened the impact of the designations by issuing a temporary General License that suspended the immediate impact of the restrictions imposed by the Entity List designations, 84 Fed. Reg. 23468 (May 22, 2019) –”Temporary General License”
    - Valid for 90 days (expires August 19, 2019)
    - Does not affect the Entity List designation – it only ‘modifies the license requirements”

Foreign Direct Investment in the US

- Foreign Direct Investment in the US has been subject to national security reviews since at least 1975
  - Executive Order by President Ford directing national security reviews of cross-border investments
- Several laws post-1975 – the Exon-Florio Amendment (1988), the Byrd Amendment (1993), and the Foreign Investment and National Security of 2007 – established a more concrete review process for the Committee on Foreign Investment in the United States ("CFIUS")
- Concerns remained, however, that existing laws did not adequately address what some believed were substantial gaps in CFIUS' jurisdiction, review process and resourcing
- Based on these concerns, Congress passed (and the President signed) into law the Foreign Investment Risk Review Modernization Act of 2018, as part of the National Defense Authorization Act of 2019, PL 115-232
  - FIRRMA reinforced CFIUS' jurisdiction over various cross-border transactions – i.e., private equity and venture capital investments, real estate transactions, bankruptcy proceedings, and joint venture investments
  - FIRRMA also codified additional factors to review when assessing the national security impact of a cross-border investment
  - FIRRMA identified a path forward for foreign investment vehicles that limit CFIUS' jurisdiction for review
  - FIRRMA established a new category of 'critical technology' – i.e., emerging or foundational technologies – and directed a new process for the identification and designation of these technologies as 'critical'

Foreign Direct Investment in the US
Why is FIRRMA Important?

- Background
  - FIRRMA's genesis
    - Driven in part by concerns included in the Section 301 Report regarding China's technology transfer practices, cybersecurity intrusions, economic espionage and trade secret theft
    - Although these concerns existed since at least 1999, China's public statements concerning concerted efforts to develop indigenous capabilities through a "Made in China 2025" policy related industries or technologies of interest to the US exacerbated the impact of the practices identified in the Section 301 report
    - Industries or technologies of concern to the US include, but are not limited to:
      - Biotechnology
      - Artificial intelligence
      - Robotics
      - Aerospace manufacturing
      - Semiconductor manufacturing
      - Nanotechnology
      - Telecommunications and information systems
      - Internet-of-Things
    - The majority of these areas coincided with China's Made in China 2025 plan to seek dominance in these areas

Foreign Direct Investment in the US

- Recent Actions and Outcomes
  - FIRRMA did not expressly identify China as a country of concern
  - Treasury issued regulations in October of 2018, effective, November of 2018, that
    - Established a pilot program for the implementation of mandatory declarations for cross-border investments that involve critical technologies and one of 27 NAICS codes identified in the regulations
    - Updated the definitions of control, US business and certain investments to highlight and address those areas where the US had a concern regarding China's direct or indirect investments in US businesses

Foreign Direct Investment in the US

- Recent Actions
  - Reports issued by the Rhodium Group, the Center for Strategic and International Studies, and other organizations (i.e., the National Venture Capital Association) indicate that FIRRMA and the US Government's policies related to trade (e.g., export controls, possible restrictions on emerging technologies, the imposition of tariffs) have adversely affected Chinese investments in the US
  - Some reports indicate that Chinese investments may have dropped by up to 80%

Foreign Direct Investment in the US

- Practical Effects
  - It appears that Chinese investments in the US continue
    - Investors are using new vehicles – tracking the roadmap provided in FIRRMA to establish investment mechanisms that are not subject to CFIUS review
    - Without Commerce's identification of emerging or foundational technologies as critical technologies, a number of cross-border investments may fall outside of CFIUS' jurisdiction – which has resulted in the continuation of Chinese investments in areas that are not yet controlled
    - While Chinese investments appear to be under greater scrutiny, it appears that all cross-border investments are subjected to more robust assessments
    - Taking foreign investment dollars affects the manner in which due diligence is conducted and what areas require a 'deeper dive' in order to determine what type of reviews or restrictions may apply

WHAT'S NEXT?

- Congress continues to develop legislative solutions
  - S. 29: Office of Critical Technologies and Security
  - S. 937: Protecting American Technology Act
  - S. 1459: China Technology Transfer Control Act of 2019
- The Executive Branch continues to issue Executive Orders and policy statements concerning the need to address the cyber related security gaps in IT and infrastructure systems as well as in the supply chain – *e.g.*, Addition to the Department of Commerce, Bureau of Industry and Security Entities List of parties that the Government has identified as national security risks (May 16, 2019)

QUESTIONS

Giovanna M. Cinelli
Washington, DC
T +1.202.739.5619
F +1.202.739.3001
giovanna.cinelli@morganlewis.com

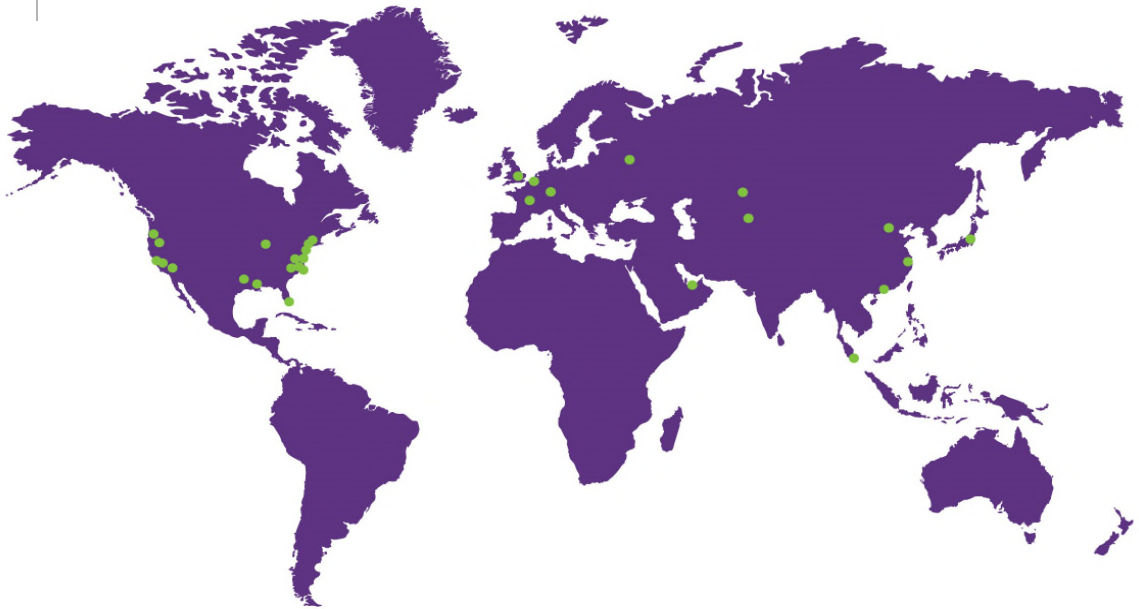
Giovanna M. Cinelli is the Firm's leader of the International Trade and National Security Practice. Throughout a career spanning over 30 years, she has represented and counseled defense, aerospace and high technology companies on a broad range of issues affecting national security, including export investigations (civil and criminal), due diligence, post-transaction cross-border compliance, Committee on Foreign Investment in the United States (CFIUS) reviews, government contracts, export policy, and licensing. She has conducted over 250 civil and criminal investigations (both unclassified and classified), addressed transactional due diligence matters in hundreds of investments, and counseled clients through the complexities of export control changes from 1992 through the present. She has negotiated complicated export enforcement settlements with the Department of State and successfully closed (without penalties) a range of directed and voluntary disclosures before the Departments of Commerce and Treasury (Office of Foreign Assets Control), as well as the Department of State. Congress considers her a subject matter expert on CFIUS. She testified on April 12, 2018 before the House Financial Services Committee on regulatory issues related to cross-border investments, national security and critical concerns involving the implementation of FIRRMA by the US. She is a frequent participant at workshops and conferences hosted by the Center for Strategic and International Studies, the Council on Foreign Relations and the Parliamentary Intelligence Forum hosted by the US Congress under Congressman Robert Pittenger's leadership. She is a member of the Firm's CFIUS Working Group, a Chambers ranked attorney and a recognized thought leader in the national security, CFIUS and export control fields.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.

THANK YOU

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.