STEVENS&BOLTON

CRITICAL THIRD PARTIES REGIME

The Bank of England (BoE), the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) (the regulators) recently ran a joint consultation on their proposals for addressing potential risks to the stability of the UK financial system arising from disruptions or breakdowns in services provided by critical third parties (CTPs).

The recently closed consultation proposed the implementation of rules to regulate CTPs that currently operate in an unregulated space.

With increasing reliance by financial services firms and financial market infrastructure entities (FMIs) on unregulated third parties there is a risk that disruption to a CTP may threaten the stability of the United Kingdom's financial system. After several significant IT failures, the Treasury Select Committee published a report in 2019 examining such failures and considering how the industry and the regulators could prevent such incidents occurring in the first place. Following the publication of that report, firms have become more reliant on cloud and other third party providers resulting in the BoE's financial policy committee to conclude in 2021 "the increasing reliance on a small number of cloud service providers and other critical third parties could increase financial stability risks without greater direct regulatory oversight of the resilience of the services they provide". Since these comments, HM treasury has worked with the regulators to address the role of critical third parties operating in the financial services sector and which we delve into further in this article.

The powers granted under the Financial Services and Markets Act 2000 (as amended) (FSMA) enable HM Treasury to designate a service provider as a CTP if it meets certain criteria. Most notably, designation would occur when the failure or disruption of services provided by that service provider would pose a risk to the stability or confidence in the UK financial system (material services).

The regulators are proposing to introduce six fundamental rules for CTPs to comply with when providing services to firms or financial market infrastructure entities (FMIs). These rules are as follows:

- **CTP Fundamental Rule 1:** A CTP must conduct its business with integrity.
- **CTP Fundamental Rule 2:** A CTP must conduct its business with due skill, care and diligence.
- **CTP Fundamental Rule 3:** A CTP must act in a prudent manner.
- **CTP Fundamental Rule 4:** A CTP must have effective risk strategies and risk management systems.

- **CTP Fundamental Rule 5:** A CTP must organise and control its affairs responsibly and effectively.
- **CTP Fundamental Rule 6:** A CTP must deal with the regulators in an open and co-operative way, and disclose to the regulators appropriately anything relating to the CTP of which they would reasonably expect notice.

The rules are broad and will apply to a CTP providing services, regardless of the materiality of such services, their location and whether or not the CTP is incorporated in the UK. While the rules are similar to the FCA's principles for businesses and the PRA's fundamental rules, the CTP fundamental rules are less extensive.

In addition to the fundamental rules, the regulators propose eight **operational risks and resilience requirements** for CTPs to abide by. Unlike the fundamental rules, these requirements would apply specifically to material services. The requirements would be as follows:

REQUIREMENT 1: GOVERNANCE

A CTP must ensure that its governance process promotes the resilience of its material services. This involves a CTP appointing a qualified employee to act as point of contact for regulators, establishing clear roles for staff involved in the delivery of material services, implementing a robust approach for service resilience and ensuring maintenance, transparency and accountability through the regular review of information provided to the regulators.

REQUIREMENT 2: RISK MANAGEMENT

A CTP must effectively manage risks against its ability to continue delivering a material service. This requirement imposes an obligation on a CTP to identify and monitor both external and internal risks, ensuring that it has implemented risk management processes that effectively manage any potential risks and that it updates its risk management processes as necessary.

REQUIREMENT 3: DEPENDENCY AND SUPPLY CHAIN RISK MANAGEMENT

A CTP must identify and manage any risks to its supply chain that could in turn have a detrimental effect on how it carries out its material services. This requirement builds on requirement 2 and seeks to ensure that a CTP manages its risks concerning its supply chain and its use of a third-party contractor.

REQUIREMENT 4: TECHNOLOGY AND CYBER RESILIENCE

A CTP will be required to ensure that any use of technology that delivers, maintains or supports a material service is resilient. This will involve implementing technology, cyber risk management and operational resilience measures, regularly testing those measures, and having in place processes and measures that reflect lessons learned and that convey information to assist risk management and decision-making processes.

REQUIREMENT 5: CHANGE MANAGEMENT

A CTP must establish policies, procedures and controls to ensure the resilience of any changes, minimising the risk of any undue disruption. Before implementing any change, a risk assessment, recording, testing, verification and approval will be essential.

REQUIREMENT 6: MAPPING

A CTP will be required to identify and document (map) all resources, including the assets and technology used to deliver, support and maintain material services provided by the CTP as well as any internal and external interconnections and interdependencies identified in respect of those services.

REQUIREMENT 7: INCIDENT MANAGEMENT

A CTP will be required to have processes in place to recover from incidents that could disrupt the material services it provides in a way that minimises the impact of such disruption. The proposal involves the maintenance and operation of a financial sector incident management playbook and the setting of a maximum tolerable level of disruption to its services.

REQUIREMENT 8: TERMINATION OF SERVICES

A CTP must have in place appropriate measures to respond to the termination of any material services it provides.

In addition to the above fundamental rules and operational risk and resilience requirements, the regulators also propose to impose on each CTP the obligation to:

- Carry out annual self-assessments detailing how it complies with the requirements.
- Conduct regular scenario testing of its ability to continue providing a material service.
- Annually test its financial sector incident management playbook.
- Share any assurance and testing information with firms and FMIs.

Insurers will undoubtedly be impacted by the proposals put forth by the regulators. The PRA carried out a survey in 2020, which found that, of the insurers surveyed, they primarily utilised cloud outsourcing to run software and access additional processing capacity or to support IT infrastructure, including for various functions, such as analytics, finance, business management, customer relationship management and file sharing. In addition, the PRA identified a high concentration of IT infrastructure provision in the cloud among insurers, predominantly limited to two providers. This high concentration would pose significant risk were there to be disruption to one of those providers.

Now that the consultation has closed, the BoE and the PRA intend to publish a draft statement of policy outlining their approach to utilising disciplinary powers. Additionally, the FCA will conduct a separate consultation on the BoE's and the PRA's statement of policy on disciplinary powers.

By implementing the proposals outlined in the consultation paper, the regulators hope to mitigate and manage any risks arising from the failure or disruption of services, ultimately safeguarding insurance policyholders and the United Kingdom's financial system.

Insurers and those operating in the financial services space must carefully review their relationships in light of the proposed requirements, especially with respect to any commercial dealings and contract negotiations with a potential CTP.

KEY CONTACTS

For further information about any of the issues raised in this guide, please contact:

Gary Parnell
Partner
T: +44 (0)1483 734269
M: +44 (0)7738 695666
E: gary.parnell@stevens-bolton.com

Saad Butt
Associate
T: +44 (0)1483 406986
M: +44 (0)7974 845305
E: saad.butt@stevens-bolton.com

STEVENS&BOLTON

Wey House, Farnham Road
Guildford, Surrey, GU1 4YD
Tel: +44 (0)1483 302264
Fax: +44 (0)1483 302254
DX 2423 Guildford 1
www.stevens-bolton.com

DEPARTMENTAL\60440150v1