American Property Casualty Insurance Association
INSURING AMERICA apci.org

APCIA Response to Financial Stability Board (FSB) Discussion Paper "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships"

January 8, 2021

The American Property Casualty Insurance Association (APCIA) appreciates the opportunity to share our views with the Financial Stability Board (FSB) on its discussion paper "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships" ("paper").

APCIA is the primary U.S. trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and across the globe. Our member groups serve customers in over 170 countries and territories around the world.

Third-party risk management is an important issue, and we welcome the promotion of public-private dialogue on this topic. Included below are APCIA's general comments and responses from a diverse insurance perspective to the four questions outlined in the paper.

General comments:

Overall, APCIA is concerned that the paper does not acknowledge or account for the *benefits* that third-party service providers (TPSPs) offer in addressing the legitimate supervisory concerns that the paper suggests are created by TPSPs. For example, regarding operational resilience, the paper does not recognize the benefits cloud service providers (CSPs) can provide in mitigating or responding to disruptions caused by a cyber event. Having a resilient business model capable of efficiently responding to and recovering from a cyber disruption is vitally important. CSPs can contribute to a client's resilience by giving clients the ability to move data from one location to another or store data in multiple locations simultaneously. CSPs have multiple data centers and servers spread around the world along with resilient data architecture and redundancies that an individual insurer could not replicate in a cost-efficient manner.

Additionally, the paper fails to differentiate between CSPs and the broader set of outsourcing providers that may be relied upon for the provision of key business functions. Insofar as CSPs present unique challenges that are not necessarily replicated in the case of other material outsourcing arrangements, we would encourage the FSB to differentiate between types of outsourcing services more clearly, and not assume that issues (for example, the concentration of risk and substitutability) that are relevant to one form of outsourcing are relevant to all forms of outsourcing. Similarly, we encourage the FSB to avoid assuming that supervisory approaches that are appropriate for one type of outsourcing are also appropriate for others.

Regarding concentration and potential systemic risks, APCIA is concerned that potential regulatory responses could compound cyber security risks. For instance, FI reporting and regulator mapping intended to address concentration risks could create data and system descriptions that could cause threat actors to target FIs or TPSPs, and if the information is obtained, leverage the mapping to launch a sophisticated supply chain and other cyber attacks.

The paper also does not reference the importance of Service Level Agreements (SLAs) in outsourcing contracts with CSPs. For migration of critical business applications to CSPs, SLAs have to be definitive in terms of access rights and ability to run those applications in order to continue to serve customers.

Finally, to encourage consistency, the FSB should consider coordinating its activities on outsourcing with the Insurance and Private Pensions Committee (IPPC) of the Organisation for Economic Cooperation and Development (OECD), which is undertaking its review of outsourcing issues that are of relevance to the insurance sector specifically.

Question 1: What do you consider the key challenges in identifying, managing, and mitigating the risks relating to outsourcing and third-party relationships, including risks in sub-contractors and the broader supply chain?

APCIA has identified several key challenges for the FSB's consideration. First, consistent with the overall approach to cybersecurity, fundamental elements of effective third-party risk management are proportionality and risk-based supervision principles. Unfortunately, these essential principles are lacking in many requirements relating to TPSPs, including CSPs.

Some supervisors may also focus more on new risks arising from cloud migration than on the operational risks of maintaining a legacy technology stack.

Regarding the challenges posed by audit requirements, CSPs and other TPSPs may be subject to dozens of (internal or external) audits on the same or similar topics, conducted on behalf of different clients, in addition to the self-certification or third-party certifications that CSPs themselves may undertake. The vast array of duplicative, uncoordinated audits can be onerous and reduce the efficiency or technological developments of a TPSP.

Further, companies report that some TPSPs are unwilling to provide them with the requested powers of access or audit to enable them to comply readily with the requirements placed on them by FI supervisors. TPSPs, particularly large CSPs or similar entities such as trade repositories, have indicated that their cybersecurity or operational integrity may be compromised by exposing highly sensitive information – including details of their cyber-defenses – to multiple outside parties.

Data localization and data nationalism also present enormous challenges to the successful utilization of TPSPs. Data localization rules that require data to be stored locally and/or that certain domestic software be used often impose costs without a commensurate increase in

regulatory certainty. Furthermore, they can exacerbate cybersecurity issues, as the onshoring of data can prevent insurers and TPSPs from mitigating the risk through geographic diversification of data storage. Related, there are significant challenges facing cross-border data transfers from the European Economic Area to third-country jurisdictions in light of the Schrems II decision, and subsequent changes proposed to transfers by the European Data Protection Board and European Commission. Domestic software's mandated use can also prevent TPSPs and insurers from having consistent cybersecurity programs globally, and intentional "backdoors" inserted by governments can weaken cyber defenses.

Question 2: What are possible ways to address these challenges and mitigate related risks? Are there any concerns with potential approaches that might increase risks, complexity, or costs?

Overall, government authorities should be encouraged to adopt proportionate and risk-based approaches to third-party arrangements.

Where TPSPs are entering the FI value chain via outsourcing arrangements and are offering, providing, intermediating, or facilitating the choice or delivery of an FI product or service, it may be worth exploring an activities-based, rather than entity-based, approach to supervision. For example, authorities could adopt a model that does not foist all the third party's regulatory responsibilities on the insurer but involves more shared responsibility between insurers and TPSP.

Regarding the duplicative audit and access requirements, there are possible workarounds that would depend on supervisory flexibility and creativity. There may be actions the FSB can take to encourage legislators and regulators to facilitate joint industry audits or other collaborative reviews of TPSPs, to reduce the burden of duplicative information requests. Joint audits should be based on standards that are made uniform to the greatest extent practicable.

Question 3: What are possible ways in which financial institutions, third-party service providers, and supervisory authorities could collaborate to address these challenges on a cross-border basis?

Facilitating platforms for cross-border public-private dialogue can help arrive at meaningful and workable solutions.

Specific to data localization challenges, supervisory and other governmental authorities in various jurisdictions can help address the problems created by data localization that exacerbate TPSP issues by making clear statements opposing data localization and implementing a policy that protects the free flow of data. Examples of such approaches can be found in the Financial Services Chapter of the U.S.-Mexico-Canada Agreement (USMCA) and the U.S.-Singapore Joint Statement on Financial Services Data Connectivity.

Question 4: What lessons have been learned from the COVID-19 pandemic regarding managing and mitigating risks relating to outsourcing and third-party relationships, including risks arising in sub-contractors and the broader supply chain?

The industry continues to assess the lessons learned from the COVID-19 pandemic and the rapid switch to a work-from-home environment, but initial indications suggest that TPSPs were an important aspect of the successful deployment of operational resilience plans. As the paper notes, the pandemic may accelerate digitalization, including through cloud computing technologies. As such, we continue to evaluate TPSP management issues for efficiency, business continuity needs, risk mitigation, and management needs.

Thank you again for the opportunity to share our views on the paper. Please do not hesitate to reach out to us if we can be of any further assistance.

Staff contacts:

Stephen Simchak,
Head of International, Department Vice President, and Counsel
Steve.Simchak@APCI.org

Angela Gleason
Senior Director Cyber & Counsel
Angela.Gleason@APCI.org