31 August 2020

Pengarah,
Jabatan Pemantauan Pembayaran,
Bank Negara Malaysia,
Jalan Dato' Onn, 50480, Kuala Lumpur

Subject: Asia Internet Coalition (AIC) Comments on Merchant Acquiring Services – Exposure Draft

Dear Pengarah,

The Asia Internet Coalition (AIC) and its members wishes to express our sincere gratitude to Bank Negara Malaysia (BNM) for the opportunity to submit comments on BNM's Exposure Draft on Merchant Acquiring Services.

As an introduction, AIC is an industry association comprised of leading Internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of Internet and ICT policy issues. Our current members are Amazon, Facebook, Google, Apple, Airbnb, Expedia Group, Grab, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verzon Media), SAP and Booking.com.

First and foremost, we commend BNM for your efforts in publishing the Merchant Acquiring Service Exposure Draft. We take note that BNM is looking to expand its regulation and supervision over Qualified Acquirers and align the regulatory regime that applies to Qualified Acquirers with licensed financial institutions. We append with this letter herewith, our proposed comments and recommendations for your kind consideration, please.

We also wish to highlight that parts of the Exposure Draft *(particularly Section 20)* has followed through from the previous BNM Risk Management in Technology (RMiT) policy document. We are of the view that this section in particular maybe worth a relook and perhaps another round of consultations to better understand the operational issues related to RMIT. For your information, the AIC has previously submitted comments for the RMiT which can be accessed via this link.

We are also grateful to the BNM for upholding a transparent, multi-stakeholder approach in developing this Exposure Draft. We further welcome the opportunity to offer our inputs and insights, directly through meetings and participating in official consultations.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Comments and recommendation on the Merchant Acquiring Services – Exposure Draft

Section	Issues	Comments	Recommendation
16.5	This provision is for acquirers to require on-site inspection of service providers, including cloud service providers (CSPs). It is contrary to the BNM Outsourcing Guidelines that recognizes alternative means to exercise audit and inspection on cloud service providers. "Acquirers shall establish outsourcing agreement when engaging an outsourced party, which must be comprehensive and includes the following: c. clear provisions on access rights for the Bank and any party appointed by the acquirers to examine any activity of and/ or related to the acquirers. This shall include access to any record, file or data of the acquirers, including management information and the minutes of all consultative and decision-making processes as well as rights to enter the premises of the outsourced party to conduct examination or investigation"	This provision should expressly allow acquirers to rely on third party audit reports instead of carrying out an on-site inspection of service providers, as per Section 11.3 of the BNM Outsourcing Guidelines The requirement that CSPs must offer customers access to the premises is not consistent with a public cloud model, which is a multi-tenanted environment and where customers retain control over their data and security controls at all times. This requirement would effectively allow acquirers access to the same physical environment used by many other companies, creating security risks. Other risks include property damage and personal injury. It also contravenes internationally recognized security best practices and standards for public cloud. Possible Alternative Solution: While acquirers should have access to independent	Under Section 11.3 of the BNM Outsourcing guideline, third party reports are acceptable as an alternative for information access. We recommend amending 16.5(c) to include substantively the same provision in the BNM Outsourcing Guidelines, as set out below: "The acquirer may rely on third party certifications and reports made available by a cloud service provider to exercise its access rights under this section, provided such reliance is supported by an adequate understanding and review of the scope of the audit and methods employed by the third party, and access to the third party and service provider to clarify matters relating to the audit."

Section	Issues	Comments	Recommendation
		information about outsourced services to enable them to understand and manage relevant risks, this objective can be met by alternative audit and reporting mechanisms instead of physical audit and inspection rights. BNM can require service providers to provide regular audit reports certifying that they are meeting global security standards. This was recognized by BNM in the Outsourcing Guidelines.	
16.6	This provision requires acquirers to ensure outsourced parties, including cloud service providers, to comply to additional privacy requirements set by BNM. This does not work in a cloud services model, where security and the nature of the services operate in a standardized manner globally. "In addition to the requirements in paragraph 16.5(b), the acquirer shall ensure that the outsourced parties provide a written undertaking to the acquirers to comply with the secrecy provision pursuant to section 133 of the FSA, the Policy Document on Management of Customers Information and Permitted Disclosures issued by the Bank, and any	This requirement is not in the BNM Outsourcing Guidelines. The Guidelines have provisions on ensuring that the CSPs maintain confidentiality and we recommend changes to this provision to be in line with language in the BNM outsourcing guidelines. Generally, within the shared responsibility framework under which CSPs operate, the acquirer is the sole party that determines what information it stores and processes using the CSP's services. The acquirer also retains full control and access to such information at	We recommend amending this section as shown below. "In addition to the requirements in paragraph 16.5(b), <u>where the outsourced party will have access to documents or information relating to the affairs or account of any customer of the acquirer, the acquirer shall ensure that the outsourced party has appropriate controls in place and is effective to safeguard the security, confidentiality and integrity of any information shared with the Outsourced Party. The acquirer shall also ensure that the service provider is bound by adequate confidentiality provisions stipulated under the outsourcing agreement."</u>

Section	Issues	Comments	Recommendation
	other relevant policy documents as may be specified by the Bank."	all times. They are empowered and have the flexibility to apply additional security if required to their content that they store or process using cloud services, including measures such as anonymizing data, restricting access rights or encryption. On the other hand, as CSPs do not have visibility into customers' content, it has no control over the security controls that the acquirer has chosen to apply. CSPs can only provide an undertaking on activities and responsibilities that remain in their control. Any proposal to extend the visibility of CSPs to customer data handling would breach security and privacy best practices, and invalidate multiple security certifications.	
16.8	The requirements on subcontracting could be interpreted as being overly prescriptive, and may not be feasible to implement for hyperscale cloud service providers that provide their services on a one-to-many basis. "The requirement in paragraph 16.7 [*on compliance with all relevant regulatory requirements*] is also applicable when an outsourced party engages a	There are a range of outsourcing arrangements that service providers can enter into and service providers may use subcontractors to deliver their services in varying degrees – these situations are not identical and therefore should not be regulated in an overly prescriptive manner. Adequate controls should be imposed on	We recommend that this requirement is amended as shown below. "The requirement in paragraph 16.7 is also applicable when an outsourced party engages a subcontractor to undertake the activities that were outsourced by the acquirer, whereby the acquirer shall implement proper controls to ensure <u>the accountability of the primary outsourced party over the performance</u>

Section	Issues	Comments	Recommendation
	subcontractor to undertake the activities that were outsourced by the acquirer, whereby the acquirer shall implement proper controls to ensure that the subcontractor complies with the relevant requirements based on standards issued by the Bank to acquirers from time to time."	subcontractors commensurate with their importance and role in the delivery of the services to the acquirer. As Section 9.6 of the BNM outsourcing guidelines recognize, the key issue with subcontracting is to ensure that service providers do not diminish the ultimate responsibility of the primary service provider.	and conduct of the subcontractor in relation to the outsourcing arrangement. ~~that the subcontractor complies with the relevant requirements based on standards issued by the Bank to acquirers from time to time~~."