Bird & Bird ATMD

Cybersecurity & Singapore

Mitigation of risks posed by digitalised payments and certain financial services

July 2019

Given increased adoption of new technology for payment systems and within the financial ecosystem, the relevant authorities in Singapore have provided guidelines to mitigate cybersecurity risks. Despite adopting mitigating practices, disruptive cybersecurity events can and do occur. When such events occur, the relevant authorities have prescribed certain reporting requirements. This fifth article in our ***Cybersecurity & Singapore*** *series highlights some of the key points that providers and users of such payment or financial service need to take note of from a cybersecurity perspective.*

Reporting Requirements under the Payment Services Act ("PSA")

The PSA was read in Parliament on 19 November 2018 and is intended to: (i) consolidate two existing Acts – the Payment Systems Oversight Act (Cap. 222A) of Singapore and the Money-changing and Remittance Businesses Act (Cap. 187) of Singapore; and (ii) expand the scope of current laws to include new activities.

Entities that are regulated under the PSA either as a designated payment system or payment service provider are required to report to the Monetary Authority of Singapore ("**MAS**") as soon as practicable after the occurrence of events which may materially impair or impede the operations of such regulated entities or access to such systems.

The PSA and the relevant regulations are likely to come into effect in 2019. However, this has not been confirmed or announced by the relevant authorities as at the date of this article. There will be more clarity as to the reporting requirements and obligations of entities regulated under the PSA once the relevant guidelines and subsidiary legislations have been released.

Technology Risk Management for Financial Institutions[1]

The Technology Risk Management Guidelines ("**TRM Guidelines**"),[2] are a set of guidelines issued by MAS to provide a set of best practices to financial institutions and to provide a guide on how they should manage technology.

The TRM Guidelines provide guidance for a financial institution's board of directors. In the TRM Guidelines:

(a) the board of directors and senior management of a financial institution should establish sound and robust risk management frameworks and ensure that effective internal controls and risk management practices are implemented to achieve not only security, but reliability, resiliency and recoverability of systems;

(b) financial institutions should arrange for its employees, contractors and vendors who have access to the financial institutions' IT resources and systems to attend a comprehensive IT security awareness training program. These programs should be conducted anually and should be

[1] Financial institution has the same meaning as in section 27A(6) of the Monetary Authority of Singapore Act (Cap. 186) of Singapore.
[2] Technology Risk Management Guidelines dated June 2013.

endorsed by the financial institution's senior management.

A risk management framework should also be established to manage technology risk. Some of the key guidance in the TRM Guidelines in relation to establishing a risk management framework is as follows:

(a) maintaining a risk register to facilitate the monitoring and reporting of risk; and

(b) developing IT risk metrics to highlight systems, processes or infrastructure that have the highest risk exposure.

The TRM Guidelines also provides guidance on how financial institutions should manage its IT outsourcing risk. These include but are not limited to:

(a) the board of directors and senior management of a financial institution conducting due diligence of a service provider prior to its appointment to determine its viability, capability, reliability track record and financial position;

(b) ensuring that the agreement governing the relationship between the service provider and the financial institution clearly sets out the relevant performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility;

(c) ensuring the service provider employs a high standard of care in its security policies, procedures and controls that would be at least as stringent as the financial institution's own operations;

(d) reviewing the third party service providers policies, procedures and control on a regular basis; and

(e) ensuring the service provider establishes a disaster recovery contingency framework and clearly define its roles and responsibilities, and conducting regular training for such plans and procedures.

E-Payment User Protection

MAS has provided guidance in an e-payment guideline[3] as to its expectations of any responsible financial institution that issues or operates a protected account (as defined in the e-payment guideline). This guideline applies to any bank, non-bank credit card issuer, finance company or approved holder that issues a protected account ("**responsible FI**"). One of the purpose of the e-payment guidelines is to provide some basic protection against unauthorised transactions.

In order to prevent unauhorised transactions, a responsible FI is required to send transaction notifications to an account holder. The notification obligations of a responsible FI are as follows:

(a) transaction notification should be sent to every contact provided by the account holder;

(b) transaction notification to be made on a real time basis or on a batch basis at least once every 24 hours;

(c) in-app notifications may be used but it must be followed by an email to sms notification (as the case may be);

(d) include relevant information on the transaction authorised in the notification[4].

In addition to providing guidance for a responsible FI, MAS has also provided guidance on (i) the information that an account holder of a protected account is required to provide; and (ii) obligations of an account user.

The information that an account holder should provide are as follows:

(a) mobile number (if the account holder opts to receive transaction notifications by SMS); or

(b) email address (if the account holder opts to receive transaction notifications by email).

Once the account holder has provided the information above, the responsible FI can assume that the account holder will monitor the notifications. As such, the account holder should ensure that the information provided is complete and accurate.

An account may be used by an account holder or an authorised person ("**account user**"). Some of the key obligations of an account user are as follows:

(a) not voluntarily disclose any access code;

(b) not keep a record of any access code such that it can be misued; and

(c) if the access code is recorded, keep the record in a secure location.

The responsible FI should inform the account user of its obligations so that the account holder is aware of their obligations and can inform the account user.

In an event where an unauthorised transaction has occurred, the account holder should report[5] the event as soon as practicable to the responsible FI in the agreed manner or in a way where an acknowledgement from the repsonsible FI is received. If the account holder is unable to do so, the responsible FI may request that the account holder provide reasons for the delay.

[3] E-Payments User Protection Guidelines issued on 28 September 2018

[4] Relevant information to be included can be found in paragraph 4.4(d) of the e-payment guidelines.

[5] Relevant information that a responsible FI may request for can be found in paragraph 3.9 of the e-payment guidelines.

Conclusion

The relevant authorities in Singapore have provided a rather comprehensive guide on the minimum requirements payment and financial service providers should meet when it comes to mitigating cybersecurity risk. However, there is no doubt that advancement in the use of technology will inevitably outpace regulations and guidance from the regulators. As such, payment and financial service providers should not strive to maintain the minimum standards provided and should take it upon themselves to adapt and maintain a higher standard than prescribed as the effect of a cybersecurity event could have the potential to severely disrupt its business.

Contact Us

For queries or more information, please do not hesitate to contact any member of the Financial Services team.

Kim Kit Ow
Partner

Tel: +65 6428 9810
kimkit.ow@twobirds.com

Teck Chai Yap
Associate

Tel: +65 6428 9427
teckchai.yap@twobirds.com