Linklaters

Singapore – MAS proposes guidelines to protect users of e-payments

Summary

The Monetary Authority of Singapore ("**MAS**") recently issued a consultation paper on proposed guidelines (the "**Guidelines**") to protect users of electronic payments ("**e-payments**"). The consultation forms part of the MAS' broader initiative to modernise and streamline the existing payment services regulatory framework in Singapore. Related consultations occurred in August 2016 and November 2017.

The Guidelines aim to make e-payments transactions simpler and more secure for individuals and micro-enterprises. As such, they will help achieve the MAS' "Smart Nation" vision of wider adoption of e-payments services and deeper integration of these services into daily economic activity. The Guidelines would require financial institutions to provide individuals and micro-enterprises who hold e-payment accounts with timely notifications of e-payment transactions, and set resolution processes for unauthorised or erroneous e-payment transactions. The Guidelines would also set out responsibilities for e-payment users, including recommended security practices to protect their e-payments accounts.

This paper provides an overview of the MAS' proposals and compares key elements of the proposals with similar rules in the United Kingdom and Australia.

Key proposals

The following institutions ("**responsible FIs**") will be subject to the Guidelines:

> banks and non-bank credit card issuers under the Banking Act (Cap. 19 of Singapore);

> finance companies under the Finance Companies Act (Cap. 108 of Singapore);

> widely accepted stored value facility holders under the Payment Systems (Oversight) Act (Cap. 222A of Singapore); and

> payment services licensees that issue payment accounts under the new Payment Services Bill (when the latter commences).

The Guidelines would apply to any "**protected account**", being a payment account that (i) is held by one or more individuals or micro-enterprises (i.e. businesses employing fewer than 10 persons or with annual turnover of no more than S$1 million), (ii) is capable of having a balance of more than S$500 or is a credit facility, and (iii) can be used for e-payment transactions.

The following sections summarise the key proposals under the Guidelines.

> "Responsible FIs will need to consider any cost impact from applying the operational and liability provisions."

Liability for losses arising from unauthorised transactions

Part A of the Guidelines describes situations in which an account holder will either (i) not be liable for losses arising from unauthorised transactions, (ii) be liable only for losses up to S$100, or (iii) be liable for actual loss (capped at any applicable transaction limit or daily payment limit). These situations, the resulting types of liability and their rationale are summarised in the table below.

Liability incurred by account holder	Situation determining liability	Rationale

No liability	> fraud or negligence committed by:
	  > the responsible FI, its employee, its agent or any third party engaged by the responsible FI
	  > the merchant involved in a previous purchase transaction, or its employee or agent
	> invalidity of a relevant device (e.g. any access code), other than by reason of an account user's action
	> initiation or execution of a payment transaction prior to the account user's receipt of a relevant device (e.g. any access code) or after the responsible FI is informed of a breach or loss in respect of the protected account or device
	> the account holder showing that the account user has not contributed to the loss
	> failure by a responsible FI to comply with its duties under the Guidelines, where this has caused the loss
		Standardising "no liability" situations enhances confidence in e-payments.
		These standardised situations are aligned with those which many financial institutions already provide for in terms and conditions of payment accounts (albeit with variations from one institution to another).

Liable for an amount of no more than S$100	> misplacement of the protected account or an authentication device or access code for that account > reporting of an unauthorised transaction by an account holder to the responsible FI outside the timeline prescribed under the Guidelines, but within a period acceptable to the responsible FI, in either case where the account user's negligence contributed to the loss	This type of limited liability is common in developed jurisdictions. The liability cap of S$100 appears generally acceptable to account users and financial institutions, and serves to contain moral hazard.
Liable for actual loss (capped at any transaction limit or daily payment limit agreed between the account holder and responsible FI)	> any unauthorised transaction where the responsible FI shows that any account user's recklessness was the primary cause of the loss (including where any account holder or account user deliberately did not comply with the Guidelines) > any transaction which the account user knew of and consented to, notwithstanding that the account holder may not have consented to the transaction. This includes the situation where an account user defrauds any account holder or the responsible FI	The account holder should be liable for actual loss arising from transactions perpetuated or caused by the account user. Account users should be encouraged to exercise due diligence in using payment accounts.

Notwithstanding the above, where the account agreement or any payment account scheme specifies a lower amount for the account holder's liability in the above situations, or where the responsible FI has offered such a lower amount, that lower amount will apply.

Duties of account holders and account users

Part B of the Guidelines describes the duties of account holders and users in respect of the proper handling of their accounts and the provision of information to responsible FIs to allow an appropriate response to unauthorised transactions.

Broadly, account holders must:

> provide the responsible FI with specified contact details to allow the responsible FI to send transaction notifications to the account holder;
> monitor transaction notifications which the responsible FI sends to the account contact;
> report an unauthorised transaction to the responsible FI by the next business day from receipt of any transaction notification, or as soon as practicable if the responsible FI agrees;
> provide the responsible FI with specified information, as requested by the responsible FI, within five business days from receipt of any transaction notification for an unauthorised transaction; and
> make a police report if the responsible FI requests such a report to be made in connection with the reporting of certain unauthorised transactions.

Account users are required, in summary, to:

> protect access codes for protected accounts (e.g. codes should not be unduly disclosed to any third party or safekept in a manner that allows third-party misuse); and
> protect access to protected accounts (e.g. by installing security updates for systems used to access the account, and using strong passwords).

Duties of responsible FIs

Under Part C of the Guidelines, responsible FIs must take steps to enable account holders to monitor payment transactions and to report unauthorised or mistaken transactions to the responsible FI. These duties of responsible FIs include:

> informing account holders of their duties and those of account users and responsible FIs, either in the account agreement or by obtaining the account holder's written acknowledgement;
> sending transaction notifications with prescribed information to account holders. These must be sent by SMS or email at least once every 24 hours during the period in which a transaction is made;
> providing an onscreen opportunity for any account user to confirm the payment transaction before it is executed;
> providing account holders with a free channel to report unauthorised or erroneous transactions, and acknowledging reports made by SMS or email;
> completing the investigation of any claim made by an account holder in relation to any unauthorised transaction within 21 or, in exceptional circumstances, 45 business days of the account holder's report, and obtaining an acknowledgement of the reported investigation outcome from the account holder; and
> crediting the protected account with the total loss arising from any unauthorised transaction, regardless of whether a claim is still being investigated, unless the responsible FI has good reasons to believe that the account holder is primarily responsible for the loss and has communicated its reasons to the account holder.

Specific duties in relation to erroneous transactions

Part D of the Guidelines describes the process for dealing with payments that have been erroneously placed with or transferred to a wrong recipient. This process requires the responsible FI of the account holder and that of the wrong recipient to exchange specified information on the transaction within prescribed timeframes. It also requires the account holder to provide its responsible FI with certain information, and the responsible FI of the recipient to consult the recipient, to ensure that the transaction is appropriately handled.

Commentary

While the additional certainty introduced by the Guidelines in respect of the handling of payment transactions is to be welcomed, the Guidelines leave certain points unaddressed, some of which may be clarified through the consultation process. These include, for example:

> How are responsible FIs expected to handle cross-border payment transfers? For example, the proposed process for reversing erroneous transactions only envisages the situation where both the account holder's account and the recipient's account are held with responsible FIs in Singapore.

> Where a responsible FI refunds an unauthorised payment, must the refund also include any charges and interest payable by the account holder as a consequence of the unauthorised transaction?

> In what circumstances should an account holder be deemed to have acted recklessly? While the MAS clarifies that recklessness includes the account holder or account user deliberately not complying with any duty in Part B of the Guidelines, it would be helpful for the MAS to provide further guidance on the meaning of recklessness for the purposes of the Guidelines.

> How will the Guidelines interact with existing industry standards issued by the Association of Banks in Singapore, such as provisions on unauthorised transactions in the Code of Practice for Banks – Credit Cards?

It is to be hoped that these points will be clarified by the MAS over the course of its discussions with the industry on the Guidelines.

Position in the United Kingdom and Australia

The approach set out in the Guidelines with respect to timely notifications of payment transactions and resolution of unauthorised or erroneous transactions overlaps with the approach taken in other jurisdictions, notably the UK and Australia. Some key points of comparison with those jurisdictions are noted below.

UK

In the UK, conduct requirements in relation to payment transactions are set out principally in the Payment Services Regulations 2017 (which implement the revised Payment Services Directive), the Electronic Money Regulations 2011, and (in respect of credit agreements) the Consumer Credit Act 1974. Compliance with the UK payment services framework is monitored jointly by the Financial Conduct Authority and the Payment Systems Regulator.

While this framework functions in a similar manner to the proposed Guidelines and also sets out comprehensive requirements for the provision of information by payment services providers ("PSP") prior to and following payment transactions, there are some notable differences from the Guidelines. For example, under the UK regime:

> to be entitled to redress for unauthorised transactions, non-execution or defective or late execution of transactions, payment service users are only required to notify the PSP without undue delay, and no later than 13 months after the debit date, on becoming aware of any unauthorised or incorrectly executed payment transaction. This contrasts with the Guidelines, under which account holders must, to benefit from relevant liability caps, assist the responsible FI with its investigation of the claim and notify it within one business day of receipt of the transaction notification, or as soon as practicable if the responsible FI agrees;

> the liability provisions regarding unauthorised transactions are more explicit in allocating the burden of proof to a relevant party (in most cases, this is the PSP);

> some situations are envisaged that are not explicitly reflected in the Guidelines, e.g. force majeure (where a person cannot comply with applicable requirements due to abnormal and unforeseeable circumstances beyond the person's control); and

> the requirements regarding unauthorised transactions are statutory and legally binding (rather than issued in the form of regulatory guidance).

Australia

In Australia, the Australian Securities & Investments Commission administers the ePayments Code (the "**Code**"), which regulates consumer electronic payment transactions. The Code is a voluntary code of practice to which relevant financial institutions ("**Subscribers**") may subscribe, although Subscribers must warrant that they will comply with the Code in their terms and conditions for consumers. Requirements covered by the Code include (among others) rules for determining liability for unauthorised transactions and for recovery of mistaken internet payments. While the Code fulfils a similar role to the Guidelines, there are some notable differences between the two frameworks. For example, under the Code:

> a holder is not liable for loss arising from an unauthorised transaction that can be made using an identifier without a pass code or device;

> provisions which attribute liability for actual loss to an account holder require the Subscriber to prove the holder's contribution to the loss by applying a "balance of probability" standard;

> subscribers are not permitted to deny a user's right to claim consequential damages resulting from a malfunction of a system or equipment provided by any party to a shared electronic network (although the liability of Subscribers will be limited where the user should have reasonably been aware of the malfunction); and

> a subscriber is liable for any loss that occurs while its process for reporting unauthorised transactions is unavailable, provided that a user reports their loss within a reasonable time of the process again becoming generally available.

Implications for your business

While certain requirements under the Guidelines follow practices that some financial institutions already follow, responsible FIs will need to consider any cost impact from applying the operational and liability provisions. Acknowledging these implications, the MAS is seeking views from the insurance industry on solutions that may be offered to protect responsible FIs from the cost of refunding account holders for losses arising from unauthorised transactions.

In anticipation of the Guidelines being adopted, institutions defined as responsible FIs may wish to compare the MAS' proposals with their existing operational processes, and identify the additional implications of complying with these proposals. This may include gauging the likely impact on internal policies and procedures, payment processing systems, account terms and conditions and other customer-facing materials.

Further information

If you would like to discuss the above, feel free to contact Peiying Chua or any of your other Linklaters contacts.

Key contacts

Peiying Chua
Counsel, Singapore
Tel: +65 6692 5869
peiying.chua@linklaters.com

Hagen Rooke
Managing Associate, Singapore
Tel: +65 6692 5878
hagen.rooke@linklaters.com

Peter Fairman
Associate, Singapore
Tel: +65 6692 5818
peter.fairman@linklaters.com

Teddy Tang
Associate, Singapore
Tel: +65 6692 5725
teddy.tang@linklaters.com