SIDLEY

March 1, 2018

SIDLEY UPDATE

Monetary Authority of Singapore Consults on Proposed E-Payments User Protection Guidelines

On Feb. 13, 2018, the Monetary Authority of Singapore (MAS) issued a Consultation Paper on the Proposed E-Payments User Protection Guidelines (Consultation Paper). Under the Consultation Paper, the MAS proposes to issue a set of guidelines (Guidelines) to standardize the protection offered to individuals or micro-enterprises from losses arising from unauthorized or mistaken payment transactions.

The Guidelines are part of MAS's ongoing review of Singapore's regulatory framework for payment services. They are meant to provide general guidance and are not intended to be comprehensive or to replace or override any legislation.

Scope and Application of the Guidelines

The Guidelines will apply to banks and non-bank credit card issuers under the Banking Act, Chapter 19 of Singapore, finance companies under the Finance Companies Act, Chapter 108 of Singapore, and widely accepted stored value facility holders under the Payment Systems (Oversight) Act, Chapter 222A of Singapore.

When the Payment Services Bill[1] comes into effect, MAS intends to make the Guidelines applicable to payment services licensees that issue payment accounts.

The Guidelines will apply only to "protected accounts", which means any payment account[2] that

(i) is held in the name of one or more persons, all of whom are either individuals or micro-enterprises[3]

(ii) is capable of having a balance of more than S$500 at any one time, or is a credit facility, and

(iii) is capable of being used for electronic payment transactions.

---

[1] On Nov. 21, 2017, the MAS issued a consultation on the proposed Payment Services Bill, which sets out two parallel regulatory frameworks: (i) a new licensing framework for payment service providers and (ii) the designation framework for payment systems. A copy of this consultation is available here.

[2] "Payment account" means –

(a) any account held in the name of, or any account with a unique identifier of, one or more persons or

(b) any personalized device or personalized facility used by any person for the initiation, execution or both of payment transactions and includes a bank account, debit card, credit card and charge card.

[3] "Micro-enterprise" means any business employing fewer than 10 persons or with annual turnover of no more than S$1 million.

The Guidelines will not apply to payment transactions arising from scams[4], which will be addressed through other means such as police investigations and separate specialized guidelines that MAS may issue where suitable.

Summary of Key Proposals in the Guidelines

(For a more detailed summary of the key proposals, please refer to Annex 1 below)

Liability for losses arising from unauthorized transactions

The Guidelines provide guidance on situations that would determine the party liable for loss arising from the unauthorized transactions. For example, where there is fraud or negligence by the responsible financial institution (FI)[5], its employee, its agent or any third party engaged by the responsible FI, the account holder[6] will be exempted from liability for the loss arising from the unauthorized transaction.

On the flipside, where the account holder's recklessness was the primary cause of the loss, the account holder will be liable for the actual loss arising from the unauthorized transaction.

Where the responsible FI is unable to show that an account user's[7] recklessness was the primary cause of loss arising from any unauthorized transaction (*e.g.* where the account user was simply negligent), the account holder will be liable for no more than S$100.

Duties of account holders and account users

The Guidelines also provide guidance on the duties of account holders and account users. The non-compliance of these duties will be a factor in determining whether the account holder or the responsible FI is found to be liable for the loss arising from an unauthorized transaction.

These duties of account holders and account users include the duty to provide contact information and monitor notifications sent from the responsible FI, the duty to protect access codes, the duty to protect access to the protected account, the duty to report unauthorized transactions, and the duty to provide information on unauthorized transactions.

---

[4] Scams generally involve an intention to deceive and cheat, and where the authorized and intended payment is incidental to consummating the scam.

[5] "Responsible FI" in relation to any protected account, means any bank, non-bank credit card issuer, finance company or approved holder that issued the protected account.

[6] "Account holder" means any person in whose name a payment account has been opened or to whom a payment account has been issued, and includes a supplementary credit card holder and a joint account holder.

[7] "Account user" means –

(a) any account holder; or

(b) any person who is authorized in a manner in accordance with the account agreement, by the responsible FI and any account holder of a protected account to initiate, execute or both initiate and execute payment transactions using the protected account.

Duties of the responsible FI

The Guidelines also provide guidance on the duties of the responsible FI. The responsible FI will be liable for any loss arising from an unauthorized transaction if the loss is caused by the responsible FI's non-compliance of its duties.

These duties of the responsible FI include the duty to clearly inform account holders of user protection duties, the duty to provide transaction notifications, the duty to provide recipient credential information before the account user confirms a payment transaction, the duty to provide an appropriate reporting channel, and the duty to complete claims investigation within the specified time period.

Specific duties of the responsible FI and account holder in relation to erroneous transactions

Where an account holder has informed the responsible FI that he/she or an account user has initiated a payment transaction from a protected account such that money has been transferred to the wrong recipient (erroneous transaction), and the account holder's responsible FI has informed the wrong recipient's responsible FI for the erroneous transaction, the responsible FI of both the account holder and of the wrong recipient should make reasonable efforts to recover the sum sent in error.

The account holder should also provide the responsible FI with the relevant information in order to assist the responsible FI to recover the sums sent in error.

Invitation for Comments

Please refer to the Consultation Paper for the complete set of proposals. The deadline for comments and feedback to be submitted to the MAS is March 16, 2018. We are collating comments from clients and industry participants for submission to the MAS. If you have comments on the proposals that you would like us to submit on your behalf, please contact any of the lawyers listed below.

Annex 1

Part A: Liability for Losses Arising from Unauthorized Transactions		
	Proposal	**Summary**
1.	**Account holder to be exempted from liability for losses in certain situations**	• The account holder will not be liable for any loss arising from an unauthorized transaction if the loss arises from any of these situations (**no-liability situations**): (a) Fraud or negligence by the responsible financial institution (FI), its employee, its agent or any third party engaged by the responsible FI; (b) Fraud or negligence by a merchant from whom any account user purchases or has previously purchased goods or services, or that merchant's employee or agent; (c) A device including an authentication device[8], access code[9], unique identifier, application or system that is not valid, including one that is compromised, forged, faulty, expired or terminated, but not by reason of any account user's action; (d) A payment transaction requiring the use of an authentication device, access code or unique identifier, that is initiated or executed before any account user received the authentication device, access code or unique identifier[10]; (e) A payment transaction that was initiated or executed after the responsible FI was informed by any account holder that there has been a breach or loss of the protected account or any authentication device or access code for that protected account;

[8] "Authentication device" means any device issued by the responsible FI to the account user for the purposes of authenticating any payment transaction initiated from a payment account, including a device that is used to generate, receive or input any access code.

[9] "Access code" means a password, code or any other arrangement that the account user must keep secret, that may be required to authenticate any payment transaction or account user, and may include any of the following:

(a) personal identification number, password or code;

(b) internet banking authentication code;

(c) telephone banking authentication code;

(d) code generated by an authentication device;

(e) code sent by the responsible FI by phone text message such as SMS,

but does not include a number printed on a payment account (e.g. a security number printed on a credit card or debit card.

[10] The account user is presumed not to have received the authentication device, access code or unique identifier unless the responsible FI has an acknowledgement of receipt from the account user.

	Proposal	Summary
		(f) The account holder shows that the account user has not contributed to the loss. Where the account user has complied with its duties under Part B below, that fact will be one factor the account holder may rely on to show that the account user has not contributed to the loss; or (g) The responsible FI did not comply with any duty set out in Part C below, and such non-compliance caused the loss.
2.	**Account holder to be liable for actual loss where account user's recklessness was primary cause of loss**	• The account holder is liable for actual loss arising from an unauthorized transaction where the responsible FI shows that the account user's recklessness was the primary cause of the loss (**actual loss situations**). • Recklessness includes the situation where any account user deliberately did not comply with his/her duties under Part B below. • The account user is expected to provide the responsible FI with information that is reasonably required to determine whether the account user was reckless. • The actual loss that the account holder is liable for may be capped at any applicable transaction limit or daily payment limit that the account holder and responsible FI have agreed to.
3.	**Account holder to be liable for maximum of S$100 where account holder's recklessness was not primary cause of loss**	• Where the responsible FI is unable to show that an account user's recklessness was the primary cause of loss arising from any unauthorized transaction (**limited liability situations**), the account holder is liable for an amount of no more than S$100. • This liability cap of S$100 may apply where an account user's negligence contributed to the loss, for example: (a) misplacement of the protected account or authentication device or access code for that protected account, and (b) where any account holder reported the unauthorized transaction to the responsible FI outside the timeline set out in Part B, Proposal 4, below but within a period acceptable to the responsible FI.

	Proposal	Summary
		• If the account holder is making a report of unauthorized transactions to the responsible FI for the third or more time in any calendar year, the responsible FI may require that the account holder furnish a police report in respect of any of the situations in subparagraphs (a) and (b) above before the responsible FI begins the claims resolution process under Part C, Proposal 5, below. • Upon inquiry by the account holder, the responsible FI will be expected to provide the account holder with relevant information on the unauthorized transactions, including transaction dates, transaction timestamps and parties to the transaction, if available.
4.	**Account holder and responsible FI may agree to a lower liability cap**	• The account agreement[11] or payment account scheme rules may specify an amount for the account holder's liability in an actual loss or limited liability situation that is lower than the applicable amount or liability cap set out in the Guidelines. • The responsible FI may also offer to reduce the liability caps on a case-by-case basis where the responsible FI deems appropriate.
5.	**Application of Part A to joint accounts**	• Where the protected account is a joint account, the liability for losses set out in this Part A will apply jointly to each account holder in the joint account.

[11] "Account agreement" means the terms and conditions that the responsible FI and account holder have agreed to that govern the use of a payment account issued by the responsible FI to the account holder.

Part B: Duties of Account Holders and Account Users		
	Proposal	**Summary**
1.	**Account holder to provide contact information and monitor notifications**	• The account holder should provide the responsible FI with contact details (account contact) in order for the responsible FI to send the account holder transaction notifications in accordance with Part C below. • Where the protected account is a joint account, the account holders should jointly instruct the responsible FI on whether the responsible FI should send transaction notifications under Part C, Proposal 2, below to any or all of the account holders. • The duties of the account holders in this Part B will apply to all the account holders whom the responsible FI has been instructed to send transaction notifications to (each, a notifiable account holder). • The account holder should at a minimum provide the following contact information, which must be complete and accurate, to the responsible FI: (a) where the account holder has opted to receive transaction notifications by SMS, his/her Singapore mobile phone number, or (b) where the account holder has opted to receive transaction notifications by email, his/her email address. • The account holder is responsible for monitoring the transaction notifications sent to the account contact that s/he provided. The responsible FI may assume that the account holder will monitor such transaction notifications without further reminders or repeat notifications.
2.	**Account user to protect access codes**	• An account user should not do any of the following: (a) voluntarily disclose any access code to any third party, except as instructed by the responsible FI for any purpose including to initiate or execute any payment transaction involving the protected account; (b) disclose the access code in a recognizable way on any payment account, authentication device or container for the payment account;

	Proposal	Summary
		(c) keep a record of any access code in a way that allows any third party to easily misuse the access code; • If the account user keeps a record of any access code, s/he should make reasonable efforts to secure the record, including (a) keeping the record in a secure electronic or physical location accessible or known only to the account user, or (b) keeping the record in a place where the record is unlikely to be found by a third party.
3.	**Account user to protect access to protected account**	• The account user should at the minimum do all of the following where a device is used to access the protected account: (a) update the device's browser to the latest version available; (b) patch the device's operating systems with regular security updates; (c) install and maintain the latest antivirus software on the device; (d) use strong passwords, such as a mixture of letters, numbers and symbols; (e) enable notification alerts on transactions initiated by or executed using the protected account . • The account holder should also, where possible, follow security instructions or advice provided by the responsible FI to the account holder.
4.	**Account holder to report unauthorized transactions**	• The account holder should report any unauthorized transactions to the responsible FI by the **next business day** from receipt of any transaction notification for any unauthorized transactions, or as soon as practicable if the responsible FI agrees. • The account holder should report these unauthorized transactions by (a) reporting the unauthorized transaction in any communications channel for such purpose as set out in the account agreement, or (b) reporting the unauthorized transaction to the responsible FI in any other way and where the responsible FI acknowledges receipt of such a report.

	Proposal	Summary
5.	**Account holder to provide information on unauthorized transaction**	• The account holder should provide the responsible FI with all the following information, as requested by the responsible FI, within **five business days** from receipt of any transaction notification for any unauthorized transaction: (a) the protected account affected; (b) the account holder's identification information; (c) the type of authentication device, access code and device used to perform the payment transaction; (d) the name or identity of any account user for the protected account; (e) whether a protected account, authentication device, or access code was lost, stolen or misused, and if so; o the date and time of the loss or misuse. o the date and time that the loss or misuse was reported to the responsible FI. o the date, time and method that the loss or misuse was reported to the police. (f) where any access code is applicable to the protected account, o how the account holder or any account user recorded the access code. o whether the account holder or any account user had disclosed the access code to anyone. (g) any other information about the unauthorized transaction that is known to the account holder.
6.	**Account holder to make police report**	• The account user should make a police report if the responsible FI requests such a report to be made in accordance with Part A, Proposal 3, above.

Part C: Duties of the Responsible FI		
	Proposal	**Summary**
1.	**Responsible FI to clearly inform account holder of user protection duties**	• The responsible FI should inform every account holder of the relevant user protection duties, *i.e.*, the duties of the account holder and account user as set out in Part B above, and the duties of the responsible FI as set out in the rest of this Part C. • The responsible FI may inform the account holder of these user protection duties by (a) setting out the user protection duties in the account agreement or (b) obtaining the account holder's written acknowledgement of the user protection duties.
2.	**Responsible FI to provide transaction notifications**	• A responsible FI should provide transaction notifications to each notifiable account holder in respect of all transactions made to or from the account holder's protected account (notifiable transaction). • The transaction notification should fulfill the following criteria: (a) The transaction notification should be sent to the account holder's account contact. If the account holder has provided more than one account contact to the responsible FI, the transaction notification should be sent to the account contact selected by the account holder to receive such notifications; (b) The transaction notification should be sent at least once every **24 hours,** during which any notifiable transaction is made. In at least one of the transaction notifications for any given day, the responsible FI must consolidate every notifiable transaction made in the past 24 hours; (c) The transaction notification should be conveyed to the account holder by way of SMS or email. An in-app notification must be accompanied by an SMS or email notification that meets the deadline in sub-paragraph (b) above; (d) The transaction notification should contain o information that allows the account holder to identify the protected account such as the protected account number and to identify the recipient whether by name or by other credentials such as the recipient's account number;

	Proposal	Summary
		○ information that allows the responsible FI to later identify the account holder, the protected account, and the recipient account such as each account number or name of the account holder; ○ transaction amount, time, date and type and ○ if the transaction is for goods and services provided by a business, the trading name of the merchant and, where possible, the merchant's reference number for the transaction.
3.	**Responsible FI to provide recipient credential information before account user confirms payment transaction**	• Where transactions are made by way of internet banking, any mobile phone application or any device arranged by a responsible FI for payment transactions (including a payment kiosk), the responsible FI should provide an on-screen opportunity for any account user to confirm the payment transaction and recipient credentials before the payment transaction is executed. • The on-screen opportunity should contain the following information: (a) information that allows the account user to identify the protected account to be debited; (b) the intended transaction amount (c) credentials of the intended recipient sufficient for the account user to identify the recipient, which at minimum should be the recipient's phone number, identification number and account number or name as registered for the purpose of receiving such payments; (d) a warning to ask the account user to check the information before executing the payment transaction;
4.	**Responsible FI to provide reporting channel**	• The responsible FI should provide account holders with a reporting channel for the purposes of reporting unauthorized or erroneous payment transactions. • The reporting channel should have all these characteristics: (a) The reporting channel may be a manned phone line, phone number to receive text messages, online portal to receive text messages or a monitored email address;

	Proposal	Summary
		(b) Any person who makes a report through the reporting channel should receive a written acknowledgement of his/her report through SMS or email; (c) The responsible FI should not charge a fee to any person who makes a report through the reporting channel for the report or any service to facilitate the report; (d) The reporting channel should be available at any time every calendar day, unless it is a manned phone line, in which case that reporting channel should be available during business hours every business day.
5.	**Responsible FI to complete claims investigation within the specified time period**	• The responsible FI should complete an investigation of any claim of an unauthorized transaction made by an account holder within **21 business days** or, in exceptional circumstances, within **45 business days** of the account holder's report of the transaction as per Part B, Proposal 4, above (investigation periods). • The responsible FI should within the appropriate investigation period give each notifiable account holder a written or oral report of the investigation outcome. The responsible FI should obtain an acknowledgement (which need not be an agreement) from that account holder.
6.	**Responsible FI to credit protected account**	• The responsible FI should generally credit the account holder's protected account with the total loss arising from any unauthorized transaction, regardless of whether the investigation of any claim is still underway. • However, the responsible FI need not do so where the responsible FI has good reason to believe that the account holder (or in the case of a joint account, any account holder) is primarily responsible for the loss arising from the unauthorized transaction, and has communicated these reasons to the account holder. This includes the situation where within that calendar year the account holder has made at least two previous reports of unauthorized transactions.

Part D: Specific Duties of Responsible FI and Account Holder in Relation to Erroneous Transactions		
	Proposal	**Summary**
1.	**Responsible FI to make reasonable efforts to recover sums sent in error**	• Where (a) an account holder has informed the responsible FI in accordance with this Part D that s/he or an account user has initiated a payment transaction from a protected account such that money has been placed with or transferred to the wrong recipient (erroneous transaction) and (b) the account holder's responsible FI has informed the wrongful recipient's responsible FI of the erroneous transaction; the responsible FI of both the account holder and of the wrong recipient should make reasonable efforts to recover the sum sent in error. • Such reasonable efforts refer to (a) in respect of the responsible FI of the account holder: o Within **two business days** of receiving the necessary information from the account holder under this Part D, the responsible FI should inform the recipient FI of the erroneous transaction. o Within **seven business days** of informing the recipient FI, the responsible FI should ask the recipient FI for the recipient's response and provide its account holder with any new relevant information to allow its account holder to assess if s/he should make a police report about the erroneous transaction. (b) in respect of the responsible FI of the wrong recipient: o Within **two business days** of receiving the necessary information from the account holder's FI about any erroneous transaction, the responsible FI should; (i) inform the recipient of the erroneous transaction and all necessary information that would allow the recipient to determine if the transaction was indeed erroneous. (ii) ask the recipient for instructions on whether to send the sum sent in error back to the account holder and

	Proposal	Summary
		(iii) inform the recipient that his/her retention or use of sums transferred to him/her erroneously where s/he has had notice of the erroneous transaction is an offense under the Penal Code, Chapter 224 of Singapore. o Within **five business days** of receiving the necessary information from the account holder's FI about any erroneous transaction, the responsible FI should (i) ask the recipient for instructions whether to send the sum sent in error back to the account holder and; (ii) inform the account holder's FI about the recipient's response, including nil responses. • The same timelines are to apply where the responsible FI is both the sending FI and the recipient FI.
2.	**Account holder to make reasonable efforts to recover sums sent in error**	• For the purposes of assisting the responsible FI to recover sums sent in error, the account holder should provide the responsible FI with any of the following information as requested by the responsible FI: (a) all the information set out in Part B, Proposal 5, above except sub-paragraphs (e), (f) and (g) (b) the recipient's unique identifier, including account number, identification number, name or other credentials entered by the account user; (c) the date, time, amount and purpose of the erroneous transaction insofar as such information is known to the account user.

If you have any questions regarding this update, please contact the Sidley lawyer with whom you usually work or

Han Ming Ho
Partner
hanming.ho@sidley.com
+65 6230 3966

Yuet Ming Tham
Partner
yuetming.tham@sidley.com
+65 6230 3969 / +852 2509 7645

Josephine Law
Counsel
jlaw@sidley.com
+65 6230 3916

John Casanova
Partner
jcasanova@sidley.com
+44 20 7360 3739

Privacy and Cybersecurity Practice

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes lawyers experienced in regulatory compliance, litigation, financial institutions, healthcare, EU regulation, IT licensing, marketing counsel, intellectual property and criminal issues. Sidley provides services in the following areas:

- Privacy and Consumer Protection Litigation, Enforcement and Regulatory Compliance
- Data Breach, Incident Response and Cybersecurity Advice, Response and Litigation
- Global Data Protection, International Data Transfer Solutions and Cross-Border Issues
- Corporate Data Protection, Compliance Programs and Information Governance Assessments
- FTC and State Attorney General Investigations of Unfair or Deceptive Acts and Practices
- Cloud Computing, Social Media, Online Advertising, Internet of Things, E-Commerce and Internet Issues
- EU, China, Japan, Singapore, Hong Kong and other International Data Protection and Compliance Counseling
- Gramm-Leach-Bliley and Financial Privacy
- HIPAA and Healthcare Privacy
- Communications Law and Data Protection
- Workplace Privacy and Employee Monitoring
- Website Policies, Online Trademarks and Domain Name Protection
- Records Retention, Electronic Discovery and Defensible Deletion
- Governmental Access and National Security

Banking and Financial Services Practice

The Banking and Financial Services Practice group offers counseling, transaction and litigation services to domestic and non-U.S. financial institutions and their holding companies, as well as securities, insurance, finance, mortgage, and diversified companies that provide financial services. We also represent all sectors of the payments industry, including payment networks and processors, money transmitters, and payors and payees in various systems. We represent financial services clients before the U.S. Department of the Treasury, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau and state regulatory agencies, as well as financial services regulators in other jurisdictions where we have offices. In addition, we represent clients before the United States Supreme Court, other federal courts and state courts.

Investment Funds, Advisers and Derivatives Practice

Sidley has a premier, global practice in structuring and advising investment funds and advisers. We advise clients in the formation and operation of all types of alternative investment vehicles, including hedge funds, fund-of-funds, commodity pools, venture capital and private equity funds, private real estate funds and other public and private pooled investment vehicles. We also represent clients with respect to more traditional investment funds, such as closed-end and open-end registered investment companies (i.e., mutual funds) and exchange-traded funds (ETFs). Our advice covers the broad scope of legal and compliance issues that are faced by funds and their boards, as well as investment advisers to funds and other investment products and accounts, under the laws and regulations of the various jurisdictions in which they may operate. Our practice group consists of approximately 120 lawyers in New York, Chicago, London, Hong Kong, Singapore, Shanghai, Tokyo, Los Angeles and San Francisco. In Asia, our practice includes Singapore, U.S., English, Hong Kong and Japanese-qualified lawyers. For further information on our Investment Funds, Advisers and Derivatives practice, please contact the co-heads of Sidley's Asia Investment Funds practice: Han Ming Ho, Singapore (+65 6230 3966, hanming.ho@sidley.com), or Effie Vasilopoulos, Hong Kong (+852 2509 7860, evasilopoulos@sidley.com).