E-PAYMENTS USER PROTECTION GUIDELINES

INTRODUCTION

- The aim of these Guidelines is to establish a common baseline protection offered by our Bank on a business-as-usual basis to individuals or sole proprietors from losses arising from unauthorized transactions, or erroneous transactions from the protected accounts of these account holders.

- These Guidelines provide general guidance, and are not intended to be comprehensive nor replace or override any legislative provisions.

DEFINITIONS

- For the purpose of these guidelines:

"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 Bank by phone text message such as Short Message Services ("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).

"Account agreement" means the terms and conditions that the Bank and account holder have agreed to that governs the use of a payment account issued by the Bank to the account holder;

"Account contact" means the contact information that the account holder provided the Bank under paragraph 3.1;

"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 Bank and any account holder of a protected account, to initiate, execute or both initiate and execute payment transactions using the protected account;

"authentication device" means any device that is issued by the Bank 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;

"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 joint account holder and a supplementary credit card holder;

"Bank" has the same meaning as in section 2(1) of the Banking Act (Cap. 19);

"Currency" means currency notes and coins which are legal tender in Singapore or a country or territory other than Singapore;

"Digital payment token" has the same meaning given by section 2(1) of the Payment Services

Act 2019;

"e-money" has the same meaning given by section 2(1) of the Payment Services Act 2019;

"Finance company" has the same meaning as in section 2 of the Finance Companies Act (Cap. 108);

"High-risk activities" include, but are not limited to—

(a) adding of payees to the account holder's payment profile;
(b) increasing the transaction limits for outgoing payment transactions from the payment account;
(c) disabling transaction notifications that the Bank will send upon completion of a payment transaction; and
(d) change in the account holder's contact information including mobile number,
email address and mailing address.

"Money" includes currency and e-money but does not include digital payment tokens;

"Non-bank credit card issuer" means a person who is granted a license under section 57B of the Banking Act (Cap. 19);

"Payment account" has the same meaning given by section 2(1) of the Payment Services Act 2019;

"payment transaction" means the placing, transfer or withdrawal of money, whether for the purpose of paying for goods or services or for any other purpose, and regardless of whether the intended recipient of the money is entitled to the money, where the placing, transfer or withdrawal of money is initiated through electronic means and where the money is received through electronic means;

"Protected account" means any payment account that—

(a) is held in the name of one or more persons, all of whom are either individuals or sole proprietors;
(b) is capable of having a balance of more than S$1,000 (or equivalent amount expressed in any other currency) at any one time, or is a credit facility;
(c) is capable of being used for electronic payment transactions; and
(d) where issued by a relevant payment service provider is a payment account that stores specified e-money.

"Relevant exempt payment service provider" means any exempt payment service provider under section 13(1)(a) to (d) of the Payment Services Act 2019 that provides account issuance services where each payment account issued stores e-money;

"relevant payment service provider" means any major payment institution as defined in section 2(1) of the Payment Services Act 2019 that has in force a license that entitles it to carry on a business of providing account issuance services or any relevant exempt payment service provider;

"Bank" in relation to any protected account, means any bank, non-bank credit card issuer, finance company or relevant payment service provider that issued the protected account;

"Sole proprietor" means any business owned by an individual where the owner is personally liable for debts and losses of the business;

"Specified e-money" has the same meaning given by section 2(1) of the Payment Services Act 2019;

"Transaction notification threshold" means—

(a) the threshold for transaction alerts set by the account holder; or

(b) if the account holder did not set any threshold for transaction alerts, the default industry-baseline transaction notification threshold.

"Unique identifier" means a combination of letters, numbers or symbols specified by the Bank to the account holder and is to be provided by the account user in relation to a payment transaction in order to identify unambiguously one or both of—

(a) any person who is a party to the payment transaction;

(b) any person's payment account;

"Unauthorized transaction" in relation to any protected account, means any payment transaction initiated by any person without the actual or imputed knowledge and implied or express consent of an account user of the protected account. This includes "seemingly authorized transactions" as defined in the Guidelines to the Shared Responsibility Framework.

The following are examples of payment transactions that do not fall within the scope of unauthorized transactions:

(a) The account user knew of and intended to make the payment transaction, notwithstanding that the transaction could have arisen as a result of falling victim to a scam (e.g., e-commerce, government-official impersonation, job, investment or love scams);

(b) The transaction was performed by a person as a result of the account holder sharing access and usage of their devices with the person, or storing the person's biometrics identities on their devices. The account holder is deemed to have consented to the use of his account by this person.

- **The expressions used in these Guidelines shall, except where expressly defined in these Guidelines, have the same meanings as in the applicable Acts in which the expressions are referred to or used.**

1. Account holder to provide contact information, opt to receive all outgoing transaction notifications and monitor notifications

- The account holder of a protected account should provide the Bank with contact information as required by the Bank in order for the Bank to send the account holder notification alerts for transactions, activation of digital security token and the conduct of high-risk activities. Where the protected account is a joint account, the account holders should jointly give instructions to the Bank on whether the Bank should send transaction notifications to any or all the account holders*. The duties of the account holders in this section will apply to all the account holders that the Bank has been instructed to send transaction notifications to.

  **At present, notifications will be sent to the primary account holder only by SBI Singapore.*

- The account holder should at a minimum provide the following contact information which must be complete and accurate, to the Bank:

(a) Where the account holder has opted to receive notification alerts by SMS, his Singapore mobile phone number; or

(b) Where the account holder has opted to receive notification by email, his email address.

- It is the account holder's responsibility to enable notification alerts on any device used to receive notification alerts from the Bank, to opt to receive notification alerts via SMS, email or in-app/push notification for all outgoing payment transactions (of any amount that is above the transaction notification threshold), activation of digital security token and the conduct of high-risk activities made from the account holder's protected account, and to monitor the notification alerts sent to the account contact. The Bank may assume that the account holder will monitor such notification alerts without further reminders or repeat notifications.

2. Account user to protect access codes (passwords)

- An account user of a protected account should not do any of the following:

(a) voluntarily disclose any access code (password) to any third party, including the staff of any Bank;

(b) disclose the access code (password) in a recognizable way on any payment account, authentication device, or any container for the payment account; or

(c) Keep a record of any access code (password) in a way that allows any third party to easily misuse the access code (password).

- If the account user keeps a record of any access code (password), 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; and

(b) keeping the record in a place where the record is unlikely to be found by a third party.

3. Account user to secure access to protected account

- An account user of a protected account should at the minimum do the following where a device is used to access the protected account:

(a) download the Bank's mobile application(s) only from official sources[1];

(b) update the device's browser[2] to the latest version available;

(c) patch the device's operating systems[3] with regular security updates provided by the operating system provider;

(d) install and maintain the latest anti-virus software on the device, where applicable[4];

(e) use strong passwords, such as a mixture of letters, numbers and symbols or strong authentication methods made available by the device provider such as facial recognition or fingerprint authentication methods;

(f) not root or jailbreak the devices used; and

- not download and install applications from third-party websites outside official sources ("**sideload apps**"), in particular unverified applications which request device permissions that are unrelated to their intended functionalities. An account holder should inform all account users of the security instructions or advice provided by the Bank to the account holder.

- An account user should where possible follow security instructions or advice provided by the Bank to the account holder.

4. Account user to read content sent with access codes before completing payment transactions or high-risk activities

- An account user of a protected account should read the content of the messages containing the access codes[5] and verify that the stated recipient or activity is intended prior to completing transactions or high-risk activities.

1 Examples: Apple App Store, Google Play Store
2 Examples: Chrome, Safari, Internet Explorer, Firefox
3 Examples: Windows operating system (OS), Macintosh OS, iOS, Android OS
4 Examples: periodic updates, patches, version releases initiated by the antivirus software providers from time to time.[9]

5 Examples include one-time passwords sent via SMS or equivalent push notifications via the official mobile application of the Bank.

5. Account user to refer to official sources to obtain website addresses and phone numbers

- An account user of a protected account should refer to official sources, e.g., the MAS Financial Institutions Directory ("FID")[6], and the Bank's mobile application or the back of cards, e.g. credit card, debit card or charge card ("official sources") to obtain the website addresses and phone numbers ("contact details") of the Bank.

- To contact the Bank, an account user should use the contact details that were obtained from official sources.

- An account user should not click on links or scan Quick Response codes ("**QR codes**") purportedly sent by the Bank unless he is expecting to receive information on products and services via these links or QR codes from the Bank. The contents of these links or QR codes should not directly result in the account holder providing any access code or performing a payment transaction or high-risk activity.[7]

6. Account user to understand the risks and implications of performing high-risk activities

- An account user of a protected account should read the risk warning messages sent by the Bank before proceeding to confirm the performance of high-risk activities.

- If an account user does not understand the risks and implications of performing high-risk activities, he should access the Bank's website for more information on these activities or contact the Bank prior to performing these activities. When the account user proceeds to perform the high-risk activities, he is deemed to have understood the risks and implications as presented by the Bank.

7. Account holder to report unauthorised activities on his protected account

- The account holder of a protected account should report any unauthorised activity to the Bank as soon as practicable, and no later than **30 calendar days** after receipt of any notification alert for any unauthorized activity, e.g., transactions, high-risk activities, and the activation of a digital security token, that has not been initiated by the account holder or with the account holder's consent.

- Where the account holder is not able to report the unauthorized activity to the Bank as soon as he receives any notification alert for any unauthorized activity or within the time period, the account holder should, if the Bank so requests, provide the Bank with reasons for the delayed report.

---

6 Website link: https://eservices.mas.gov.sg/fid.

7 Such links are only to provide information and could be part of regulatory requirements, such as Terms and Conditions, product description, steps to execute a transaction and fact sheet for investment products.

- The account user can report the unauthorized transaction to the Bank through following communication channel;

a) By calling on our Hotline: 1800-724 7464 (S-B-I-S-I-N-G)/800-101-2333 (24 hrs).
b) Email contactus@sbising.com, helpdesk@sbising.com
c) Branches during business hours only.

8. Account holder to activate self-service feature ("kill switch/temporary locking of account") provided by the Bank promptly to block further mobile and online access to the protected account

- The account holder of a protected account should activate the kill switch/ Temporary Blocking of Account provided by the Bank to block further mobile and online access to the protected account, as soon as practicable, after he is notified of any unauthorized transactions and has reason to believe that the account has been compromised, or if he is unable to contact the Bank.

9. Account holder to provide information on unauthorized transaction

- The account holder of a protected account should within a reasonable time provide the Bank with the following information as requested by the Bank in the form attached in the annexure-I of this document:

(a) the protected account(s) affected, including the account holder's affected accounts with other FIs if any;
(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:
  i. the date and time of the loss or misuse,
  ii. the date and time that the loss or misuse, was reported to the Bank, and
  iii. 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,
  i. how the account holder or any account user recorded the access code, and
  ii. whether the account holder or any account user had disclosed the access code to anyone; and
(g) any other relevant information about the unauthorised transaction that is known to the account holder, such as:

i. a description of the scam incident, including details of the communications with the suspected scammer(s);
ii. details of the remote software downloaded (if any) as instructed by the scammer(s);
iii. whether the account holder has received any OTPs and/or transaction notifications sent by the Bank, and where applicable/possible a confirmation from telecommunication operators to verify the receipt status only if the account holder is able to obtain it; and
iv. suspected compromised applications (if any) in the account user's device.

10. Account holder to make police report

- The account holder of a protected account should make a police report as soon as practicable if the Bank requests such a report to be made to facilitate its claims investigation process, or if the account holder suspects that he is a victim of scam or fraud.

- The account holder should cooperate with the Police and provide evidence[8], as far as practicable. The account holder should also furnish the police report to the Bank within 3 calendar days of the Bank's request to do so, in order to facilitate the Bank's claims investigation process.

---

8 For example, consumer can furnish his mobile device to the Police for forensics investigation.

1. Account holder is liable for actual loss

- The account holder of a protected account is liable for actual loss arising from an unauthorised transaction where any account user's recklessness[9] was the primary cause of the loss. Recklessness would include the situation where any account user deliberately did not comply with the instructions mentioned in the above section. The account user is expected to provide the Bank with information the Bank reasonably requires to determine whether any account user was reckless. The actual loss that the account holder is liable for in this paragraph is capped at any applicable transaction limit or daily payment limit that the account holder and Bank have agreed to.

- For the avoidance of doubt, where any account user knew of and consented to a transaction ("**authorised transaction[10]**"), such a transaction is not an unauthorised transaction, notwithstanding that the account holder may not have consented to the transaction. This would also include the situation where any account user acts fraudulently to defraud any account holder or the Bank. The account holder of a protected account is liable for all authorised transactions up to any applicable transaction limit or daily payment limit that the account holder and Bank have agreed to.

2. Account holder is not liable for any loss

Loss resulting from any action or omission by the Bank

- The account holder of a protected account is not liable for any loss arising from an unauthorised transaction if the loss arises from any action or omission by the Bank and does not arise from any failure by any account user to comply with any duty in Section above.

---

9 Examples of conduct that constitute recklessness and could lead to losses from unauthorised transactions include:

a) storing access code in a manner that can be easily accessed by any third party;
b) knowingly sharing or surrendering access codes to non-account users, resulting in completed transactions;
c) ignoring notifications, alerts or warnings from the Bank;
d) following instructions of third parties to open new bank or card accounts without a reasonable basis;
e) retaining sideloaded apps which are unverified or request device permissions that are unrelated to their intended functionalities; and
f) selecting a numeric or alphabetical access code that is easily recognisable, such as one which represents their birth date, or part of their name, if the Bank has:
   - specifically instructed the account holder not to do so, and
   - warned the account holder of the consequences of doing so.

10 Please refer page no 4 for examples of authorised transactions.

- Any action or omission by the Bank includes the following:

  (a) fraud or negligence by the Bank, its employee, its agent or any outsourcing service provider contracted by the Bank to provide the Bank's services through the protected account;

  (b) non-compliance by the Bank or its employee with any requirement imposed by the Authority on the Bank in respect of its provision of any financial service;

Loss resulting from any action or omission of any independent third party

- The account holder of a protected account is not liable for the first $1,000 of loss arising from an unauthorised transaction, if the loss arises from any action or omission by any third party and does not arise from any failure by any account user to comply with any duty in above-mentioned Section.

3. Agreement to reduce account holder's liability

- Where the account agreement specifies a lower amount for the account holder's liability in the same situations described in this Section, the Bank should fulfil its obligation to all account holders under the account agreement.

- The Bank may offer to reduce the account holder's liability specified in this Section on a case by case basis, where the Bank deems it to be appropriate to offer such a lower amount to the account holder.

4. Application of this section to joint accounts

- Where the protected account is a joint account, the liability for losses set out in this Section apply jointly to each account holder in a joint account.

----------***----------

***Source**: The above user guidelines have been extracted from MAS circular on E payments User Protection Guidelines updated on 24/10/2024. In case of any update/amendment by MAS in the source document, the same would be applicable here as well.*

Annexure -I

To submit any claim for disputed transactions, kindly fill in the complete form and submit to any of our branches or through email at helpdesk.sbising.com and contactus@sbising.com.

SBI Singapore

E PAYMENT TRANSACTION DISPUTE FORM

DATE	D	D	M	M	Y	Y	Y	Y

Transaction Account No. (Protected Account)														

To
SBI Singapore

I/ We wish to raise dispute in respect of above affected account for E-Payment as per following information:

Primary Account Holder's Identification	:	Name	Full Name		
		ID Type	ID Number		
Joint Account Holder's Identification	:	Name	Full Name		
		ID Type	ID Number		
If used by any user of account, Name & Identity of the User	:	Name	Full Name		
		ID Type	ID Number		
The type of authentication device, access code and device used to perform the payment transaction	:	Pl specify type of device used for disputed E- payment			
		Authentication Device			
		Access Code			
		Device			
If authentication device/ access code was lost/ misused, Please advise details	:	Date and time it was lost	Date		Time
		Date & time it was reported to Bank	Date		Time
		Date & time and method it was reported to Police.	Date	Time	Method
Recording/ safekeeping of Access Code	:	How was the Access Code Recorded			
		Whether it was disclosed to anyone	Pls Tick	Yes	No
Any other relevant information	:				

Note: Please read the Declaration on Page 2 carefully and sign at the specified place.

Page 1/2

SBI Singapore

E PAYMENT TRANSACTION DISPUTE FORM

DECLARATION

1. I/ We confirm and undertake that I/we have read and understood the MAS E-payment User Protection Guidelines available at MAS website. A link to the guidelines is displayed under News & Announcements section of SBI website: https://www.sbising.com
2. I/ We understand that as users we have to ensure that our contact details are up to date with the Bank; I/ we have to always monitor our notifications; we need to report any unauthorized transactions promptly to Bank and that I/ we have to keep my/ our passcodes safe.
3. The report to Bank will be made through Helpline/ Email/ Personal visit to any of our branches and will ensure for Bank's acknowledgement of the receipt of such report.
4. I/we understand that Bank may complete an investigation of any relevant claim **within 21 business days for straightforward cases** or **45 business days for complex cases**. I/ we will provide all information required by Bank in the process of this investigation. If investigation requires from me/ us to make a police report to facilitate its claims investigation process, I/ we will arrange for the same.
5. I/we understand that I/we are liable for actual loss arising from an unauthorised transaction where any account user's recklessness was the primary cause of the loss. I/we are expected to provide the bank with information the Bank reasonably requires to determine whether any account user was reckless.

SIGNATURE			
	FIRST/ SOLE HOLDER	SECOND HOLDER	THIRD HOLDER

For Bank's Use

Dispute Claim Form Received on	:	Date	Time
Dispute Claim Form sent to Back Office on	:	Date	Time
Additional information requested from Customer on	:	Date	Time
Additional information received from Customer on	:	Date	Time
Dispute Claim Settled on	:	Date	Time
Disposal Remarks	:		

Branch official _____ Signature_____

Page 2/2