

E-PAYMENTS USER PROTECTION

GUIDELINES

1. INTRODUCTION

1. 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 unauthorised transactions, or erroneous transactions from the protected accounts of these account holders.
2. These Guidelines provide general guidance, and are not intended to be comprehensive nor replace or override any legislative provisions. They should be read in conjunction with the provisions of the relevant legislation, the subsidiary legislation made under the relevant legislation, as well as written directions, notices, codes and other guidelines that MAS may issue from time to time pursuant to the relevant legislation and subsidiary legislation.

2. DEFINITIONS

1. 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 authorised 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” means State Bank of India, Singapore Branch ("SBI SG");

“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 1967;

“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 1970;

“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;

“Responsible FI” 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;

“Unauthorised 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 authorised 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 unauthorised 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 biometric identities on their devices. The account holder is deemed to have consented to the use of his account by this person.

2. 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.

3. DUTIES OF ACCOUNT HOLDERS AND ACCOUNT USERS

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

- a. 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 holders¹. The duties of the account holders in this paragraph will apply to all the account holders that the Bank has been instructed to send transaction notifications to.
- b. The account holder should at a minimum provide the following contact information which must be complete and accurate, to the Bank:
 - i. Where the account holder has opted to receive notification alerts by SMS, his Singapore mobile phone number; or
 - ii. Where the account holder has opted to receive notification by email, his email address.
- c. 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

- a. An account user of a protected account should not do any of the following:
 - i. voluntarily disclose any access code to any third party, including the staff of any Bank;
 - ii. disclose the access code in a recognisable way on any payment account, authentication device, or any container for the payment account; or
 - iii. keep a record of any access code in a way that allows any third party to easily misuse the access code.
- b. If the account user keeps a record of any access code, he should make reasonable efforts to secure the record, including:
 - i. keeping the record in a secure electronic or physical location accessible or known only to the account user; and

¹ The availability of notifications to joint account holders, is subject to the Bank's prevailing policies, procedures and system capabilities. Customers should contact the Bank directly for the latest information and/or confirmation regarding the joint account notification arrangements, including to update the number of joint account holder(s) that can receive the notification besides the primary / main account holder.

- ii. 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

- a. An account user of a protected account should at the minimum do the following where a device is used to access the protected account:
 - i. download the Bank's mobile application(s) only from official sources;²
 - ii. update the device's browser³ to the latest version available;
 - iii. patch the device's operating systems⁴ with regular security updates provided by the operating system provider;
 - iv. install and maintain the latest anti-virus software on the device, where applicable⁵;
 - v. use strong access codes, 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;
 - vi. not root or jailbreak the devices used; and
- b. 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.
- c. 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

- a. An account user of a protected account should read the content of the messages containing the access codes⁶ and verify that the stated recipient or activity is intended prior to completing transactions or high-risk activities.

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

- a. An account user of a protected account should refer to official sources, e.g., the MAS Financial Institutions Directory ("FID"),⁷ 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.
- b. To contact the Bank, an account user should use the contact details that were obtained from official sources.

² Examples: Apple App Store, Google Play Store

³ Examples: Chrome, Safari, Internet Explorer, Firefox

⁴ Examples: Windows operating system (OS), Macintosh OS, iOS, Android OS

⁵ Examples: periodic updates, patches, version releases initiated by the antivirus software providers from time to time.

⁶ Examples include one-time passwords sent via SMS or equivalent push notifications via the official mobile application of the Bank.

⁷ Website link: <https://eservices.mas.gov.sg/fid>.

- c. 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.⁸

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

- a. 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.
- b. 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

- a. 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 unauthorised 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.
- b. Where the account holder is not able to report the unauthorised activity to the Bank as soon as he receives any notification alert for any unauthorised activity or within the time period set out in paragraph 3.7 above (i.e., no later than 30 calendar days), the account holder should, if the Bank so requests, provide the Bank with reasons for the delayed report.
- c. The account user can report the unauthorised transaction to the Bank By calling on our Hotline at 1800-724 7464 (S-B-I-S-I-N-G) / 800-101-2333 (24 hrs hotline).

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

- a. The account holder of a protected account should activate the kill switch/ temporary locking 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 unauthorised 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 unauthorised transaction

⁸ 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.

- a. 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 Annexure I of this document:
 - i. the protected account(s) affected, including the account holder's affected accounts with other FIs if any;
 - ii. the account holder's identification information;
 - iii. the type of authentication device, access code and device used to perform the payment transaction;
 - iv. the name or identity of any account user for the protected account;
 - v. whether a protected account, authentication device, or access code was lost, stolen or misused and if so:
 1. the date and time of the loss or misuse,
 2. the date and time that the loss or misuse, was reported to the Bank, and
 3. the date, time and method that the loss or misuse, was reported to the police;
 - vi. where any access code is applicable to the protected account,
 1. how the account holder or any account user recorded the access code, and
 2. whether the account holder or any account user had disclosed the access code to anyone; and
 - vii. any other relevant information about the unauthorised transaction that is known to the account holder, such as:
 1. a description of the scam incident, including details of the communications with the suspected scammer(s);
 2. details of the remote software downloaded (if any) as instructed by the scammer(s);
 3. 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
 4. suspected compromised applications (if any) in the account user's device.

10. Account holder to make police report

- a. 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.
- b. The account holder should cooperate with the Police and provide evidence,⁹ 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.

4. DUTIES OF THE BANK

1. Bank's duty to inform account holders of user protection duties, and not to send clickable links or QR codes via email or SMS, or phone numbers via SMS to account user

⁹ For example, consumer can furnish his mobile device to the Police for forensics investigation.

- a. The Bank should inform every account holder of a protected account of the user protection duties, including providing such information on its website or mobile application, and in the terms and conditions provided to an account holder for any new protected account issued.
- b. The Bank should not send clickable links or QR codes via email or SMS to an account user of a retail protected account unless:
 - i. it is a link or QR code that only contains information for the account user and does not lead to a (i) website where the account user provides his access codes or performs any payment transaction or (ii) platform where the account user is able to download and install apps; and
 - ii. the account user is expecting to receive the email or SMS from the Bank.
- c. The Bank should not send phone numbers via an SMS to an account holder of a protected account unless the account holder is expecting to receive the SMS from the Bank.
- d. The Bank should ensure its website address is listed on MAS' FID, and that its contact details reflected on MAS' FID and other official sources are up to date.

2. Bank to impose a cooling off period when performing high-risk activities

- a. The Bank should impose a cooling off period of at least 12 hours¹⁰ where high-risk activities cannot be performed ("cooling off period"), when a digital security token is activated on a device, or when there is a login to a protected account issued by a relevant payment service provider on a new device.

3. Bank to inform account user of the risks and implications of performing high-risk activities

- a. The Bank should inform the account user of a protected account of the risks and implications of performing high-risk activities and obtain additional customer confirmation, at the point before the account holders perform the high-risk activities.

4. Bank to provide notification alerts on a real-time basis, for activation of digital security token and conduct of high-risk activities

- a. The Bank should provide notification alerts on a real-time basis, that fulfil the following criteria, to the account holder of a protected account, when his digital security token is activated and any high-risk activities are performed:
 - i. The notification alert should be sent to the account holder's existing account contact with the Bank. If the account holder has provided more than one account contact to the Bank, the notification should be sent to every account contact selected by the account holder to receive such notifications.
 - ii. The notification alert should be conveyed to the account holder by way of SMS, email or in-app/push notification.

¹⁰ If the activation of the security token is via a non-straight through process (e.g. mailing of registration code), the duration of the non-straight through process counts towards fulfilling the cooling off period.

- iii. The notification alert should contain details relevant to the digital security token provisioning and activation or high-risk activity, such as information on the payee added, new transaction limits or a change in contact details.
- iv. The notification alert should contain a reminder for the account holder to contact the Bank if the digital security token provisioning and activation or high-risk activity was not performed by the account holder.

5. Bank to provide outgoing transaction notification alerts on a real-time basis

- a. Subject to paragraph 4.6 (below), the Bank should provide transaction notification alerts that fulfil the following criteria to each account holder of a protected account that the Bank has been instructed to send transaction notification alerts to in accordance with paragraph 3.1, in respect of all outgoing payment transactions (in accordance with the transaction notification threshold) made from the account holder's protected account.
 - i. The transaction notification alert should be sent to the account holder's account contact. If the account holder has provided more than one account contact to the Bank, the transaction notification alert should be sent to every account contact selected by the account holder to receive such notifications.
 - ii. The transaction notification alert should be sent on a real-time basis for each transaction.
 - iii. The transaction notification alert should be conveyed to the account holder by way of SMS, email or in-app/push notification.
 - iv. The transaction notification alert should contain the following information, but the Bank may omit any confidential information provided that the information provided to the account holder still allows the account holder to identify the transaction as being an authorised transaction (as referred to in paragraph 5.1(b)) or unauthorised transaction.
 - 1. Information that allows the account holder to identify the protected account such as the protected account number;
 - 2. Information that allows the account holder to identify the recipient whether by name or by other credentials such as the recipient's account number;
 - 3. Information that allows the Bank to later identify the account holder, the protected account, and the recipient account such as each account number or name of the account holder;
 - 4. Transaction amount (including currency);
 - 5. Transaction time and date;
 - 6. Transaction type;
 - 7. 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.

6. Compliance with account holder's preference

- a. Notwithstanding paragraph 4.5 (above), the Bank may elect to comply with an account holder's transaction notification alert preferences. While the Bank should make available to account holders the option to receive transaction notification alerts for outgoing payment transactions made from the account holder's protected account, if the account holder instructs or has instructed the Bank otherwise, the Bank may, upon its assessment and at its sole discretion, provide notification alerts for outgoing transactions in accordance with the account holder's instructions..
- b. The Bank may make available on its website or mobile application information on how an account holder can adjust the transaction notification settings (if applicable). The Bank should explain how the liability of the account holder under paragraph 5 of this Guidelines may be affected by the account holder's transaction notification preferences and how any relevant claim by an account holder (as defined in paragraph 4.13) will be resolved. The Bank should act fairly and responsibly to the account holder at all times.

7. Incoming transaction notification alerts

- a. The Bank is encouraged to provide transaction notification alerts that fulfil the criteria set out in paragraph 4.5(a)(i) to (iv) for payments to the account holder's protected account ("incoming transaction notifications") as a matter of good practice, as incoming transaction notification alerts provide e-payment users with a fuller view of their e-payments.

8. Bank to provide a self-service feature ("kill switch") for account holder to promptly block further access to protected account

- a. The Bank should provide a kill switch for an account holder to promptly block further mobile and online access to his protected account.¹¹ This includes disallowing mobile and online payment transfers to third parties who are not authorised billers.¹² The kill switch should be made available in a prominent manner via the mobile application of the Bank, the automated teller machines ("ATMs") of the Bank, or the reporting channel provided by the Bank under paragraph 4.11 to report unauthorised transactions.
- b. The Bank should educate every account holder of a protected account how to activate this feature, and highlight the duties of the account holder in paragraph 3.8 on when they should activate this feature.

9. Bank to provide information to allow identification of payment recipient

- a. The Bank should provide the following information accompanying the access codes¹³ in the same message sent to the account user to allow the account user of a protected account to identify the payment recipient:

¹¹ Existing mobile and online banking session(s) are to be terminated as well.

¹² Examples of payment transfers to authorised billers include pre-authorised transfers such as GIRO payments to billing organisations.

¹³ Examples include one-time passwords (OTP) sent via SMS or equivalent push notifications via the official mobile application of the Bank.

- i. information that allows the account user to identify the protected account such as the protected account number;
- ii. information that allows the account user to identify the recipient whether by name or by other credentials;
- iii. the intended transaction amount (including currency); and
- iv. a warning to remind the account user not to reveal the access code to anyone.

10. Bank to provide recipient credential information

- a. Where transactions are made by way of internet banking, any mobile phone application or device arranged for by the Bank for payment transactions, including a payment kiosk, the Bank should provide an onscreen opportunity for any account user of a protected account to confirm the payment transaction and recipient credentials before the Bank executes any authorised payment transaction.
- b. The onscreen opportunity should contain the following information:
 - i. information that allows the account user to identify the protected account to be debited;
 - ii. the intended transaction amount;
 - iii. credentials of the intended recipient that is sufficient for the account user to identify the recipient, which at the minimum should be the recipient's phone number, identification number, account number or name as registered for the purpose of receiving such payments; and
 - iv. a warning to ask the account user to check the information before executing the payment transaction.

11. Bank to provide reporting channel

- a. The Bank should provide account holders of protected accounts with a reporting channel that is available at all times for the purposes of reporting unauthorised or erroneous transactions, and blocking further access via mobile and online channels to his protected account.
- b. The reporting channel should have all the following characteristics:
 - i. The reporting channel¹⁴ may be a manned phone line, phone number to which text messages can be sent, online portal to which text messages can be sent, a monitored email address, mobile application of the Bank, or the ATMs of the Bank.
 - ii. Any person who makes a report through the reporting channel should receive a written acknowledgement of his report through SMS, email, or in-app notification.
 - iii. The Bank 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.

12. Bank to implement real-time detection and blocking of suspected unauthorised transactions

- a. The Bank should have in place capabilities to detect and block suspected unauthorised transactions at all times. The Bank should also have capabilities to inquire into the

¹⁴ Account holders may also choose to report unauthorised or erroneous transactions in person at the operating premises of the Bank where practicable, subject to their operating hours.

authenticity of the suspected unauthorised transactions before allowing such transactions to be executed. The Bank should review the effectiveness of its detection parameters for suspected unauthorised transactions on an annual basis, or as and when there are material triggers.

13. Bank to assess claims and complete claims investigation

- a. The Bank should assess any claim made by any account holder in relation to any unauthorised transaction covered in paragraph 5 (“relevant claim”) for the purposes of assessing the account holder’s liability in accordance with paragraph 5. It should have a proper governance structure and investigation process, involving representatives who are independent from business units who are to carry out the above assessment.
- b. Where the Bank has assessed that the relevant claim does not fall within paragraph 5, the Bank should resolve such a claim in a fair and reasonable manner. The Bank should communicate the claim resolution process and assessment to the account holder in a timely and transparent manner.
- c. The Bank may require that any account holder furnish a police report in respect of an unauthorised transaction claim, before the Bank begins the claims resolution process. In doing so, the Bank should, upon request by the account holder, provide information on the procedure to file a police report.
- d. The Bank may request any account holder to provide information set out in paragraph 3.9. Upon enquiry by an account holder, the Bank will be expected to provide the account holder with relevant information that the Bank has of all the unauthorised transactions which were initiated or executed from a protected account, including transaction dates, transaction timestamps and parties to the transaction.
- e. The Bank should complete an investigation of any relevant claim within 21 business days for straightforward cases or 45 business days for complex cases. Complex cases may include cases where any party to the unauthorised transaction is resident overseas or where the Bank has not received sufficient information from the account holder to complete the investigation. The Bank should, within these periods, give each account holder that the Bank has been instructed to send transaction notifications to in accordance with paragraph 3.1, a written or oral report of the investigation outcome and its assessment of the account holder’s liability in accordance with paragraph 5. The Bank should seek acknowledgement (which need not be an agreement) from that account holder of the investigation report.
- f. Where the account holder does not agree with the Bank’s assessment of liability, or where the Bank has assessed that the claim falls outside of paragraph 5, the account holder and the Bank may proceed to commence other forms of dispute resolution, including mediation at the Financial Industry Disputes Resolution Centre Ltd (“FIDReC”) where the Bank is a FIDReC member.

14. Bank to credit protected account

- a. The Bank should credit the account holder's protected account with the total loss arising from any unauthorised transaction¹⁵ as soon as the Bank has completed its investigation and assessed that the account holder is not liable for any loss arising from the unauthorised transaction. The Bank should disclose this arrangement to the account holder at the time the account holder reports the unauthorised transaction to the Bank, and inform the account holder of the timeline for completing its investigation in accordance with paragraph 4.13.

15. Scheduled system downtime

- a. Where relevant, paragraphs 4.1(a), 4.2, 4.4, 4.5, 4.7, 4.8, 4.11 and 4.12 of this paragraph shall apply during a scheduled system downtime. The Bank is to ensure continued delivery of key services and alternatives, where applicable. The Bank should also ensure that scheduled system downtime is not performed during periods where high volume of transactions are expected.

5. LIABILITY FOR LOSSES ARISING FROM UNAUTHORISED TRANSACTIONS

1. Account holder is liable for actual loss

- a. The account holder of a protected account is liable for actual loss arising from an unauthorised transaction where any account user's recklessness¹⁶ was the primary cause of the loss. Recklessness would include the situation where any account user deliberately did not comply with paragraph 3 or paragraph 4 of these Guidelines. 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.

¹⁵ For the avoidance of doubt, losses arising from unauthorised transactions exclude any loss of business or profit, special, punitive, indirect or consequential loss and any other losses.

¹⁶ 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.

- b. For the avoidance of doubt, where any account user knew of and consented to a transaction (“authorised transaction”),¹⁷ 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

- a. 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 paragraph 3.
- b. Any action or omission by the Bank includes the following:
- i. 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;
 - ii. 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; and
 - iii. non-compliance by the Bank with any duty set out in paragraph 4.

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

- c. 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 paragraph 3.

3. Agreement to reduce account holder’s liability

- a. Where the account agreement specifies a lower amount for the account holder’s liability in the same situations described in this paragraph, the Bank should fulfil its obligation to all account holders under the account agreement.
- b. The Bank may offer to reduce the account holder’s liability specified in this paragraph on a case-by-case basis, where the Bank deems it to be appropriate to offer such a lower amount to the account holder.

¹⁷ Please refer to the definition of “Unauthorised transaction” in paragraph 2.1 for examples of authorised transactions.

4. Application of this paragraph to joint accounts

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

6. SPECIFIC DUTIES IN RELATION TO ERRONEOUS TRANSACTIONS

This paragraph 6 applies where an account holder or his account user initiates a payment transaction that is not a credit card, charge card or debit card transaction from a protected account, such that money has been placed with or transferred to a wrong recipient ("erroneous transaction").

1. FIs to make reasonable efforts to recover sums sent in error by the account user

- a. Where an account holder has informed the Bank in accordance with this paragraph 6 that he or an account user has initiated an erroneous transaction, and the Bank has informed the wrong recipient's FI of the erroneous transaction, the FIs of both the account holder and of the wrong recipient should make reasonable efforts to recover the sum sent in error. For the purposes of paragraph 6, "FI" in relation to any payment account means any bank, non-bank credit card issuer, finance company or relevant payment service provider that issued the payment account.
- b. For the purposes of paragraph 6.1(a), reasonable efforts means the following:
 - i. Where the FI is the FI of the account holder:
 1. within two business days of receiving the necessary information from the account holder under this paragraph, the FI should inform the wrong recipient's FI of the erroneous transaction;
 2. within seven business days of informing the recipient's FI, the FI should ask the wrong recipient's FI for the recipient's response (if not already provided) and provide the account holder with an update to allow the account holder to assess if he should make a police report about the erroneous transaction;
 3. in the event that the account holder is unable to recover the erroneously transferred funds despite the FI expending all reasonable efforts to do so, and the FI assessed that the case to be closed as a result, the FI should inform the sender of the decision and advise the sender on the next steps, which may include filing a police report.
 - ii. Where the FI is the FI of the wrong recipient:
 1. within two business days of receiving the necessary information from the account holder's FI about any erroneous transaction, the FI should: (A) inform the recipient of the erroneous transaction and all necessary information that would allow the recipient to determine if the transaction was indeed erroneous; (B) ask the recipient for instructions on whether to send the sum sent in error back to the

account holder; and (C) inform the recipient that his retention or use of sums transferred to him erroneously where he has had notice of the erroneous transaction is an offence under the Penal Code;

2. within five business days of receiving the necessary information from the account holder's FI about any erroneous transaction, the FI should: (A) ask the recipient for instructions whether to send the sum sent in error back to the account holder; and (B) inform the account holder's FI about the recipient's response, including nil responses.

2. Where the wrong recipient has noticed an erroneous transaction and requests to return the sum sent in error

- a. Where a recipient has informed his responsible FI in accordance with paragraph 6 that he has received an erroneous transaction and wishes to return the sum sent in error, the recipient's FI should make reasonable efforts to assist the recipient in doing so. Where confirmation is required from the account holder (who had made the erroneous transaction) through the account holder's FI, before the recipient's FI can return the sum sent in error, the FI of the account holder should also make reasonable efforts to facilitate the return of such sum.
- b. For the purposes of paragraph 6.2(a), reasonable efforts means the following:
 - i. Where the FI is the FI of the wrong recipient: (i) if confirmation from the account holder's FI is needed before the FI can return the sum sent in error, the FI should within two business days of receiving the necessary information from the wrong recipient under this paragraph, inform the account holder's FI of the erroneous transaction, and within seven business days of informing the account holder's FI, ask the account holder's FI for a response (if not already provided) and provide the wrong recipient with an update; (ii) if confirmation from the account holder's FI is not needed before the FI can return the sum sent in error, the FI should return the sum sent in error as soon as practicable, or no later than nine business days of receiving the necessary information from the recipient under this paragraph; (iii) in the event that the FI is unable to obtain confirmation from the account holder's FI, and the FI assessed that the case to be closed as a result, the FI should inform the wrong recipient of the decision and advise on the next steps, which may include making a police report if the funds are suspected to be illicit in nature.
 - ii. Where the FI is the FI of the account holder, and confirmation from the FI is needed before the wrong recipient's FI can return the sum sent in error, the FI should, within five business days of receiving the necessary information from the wrong recipient's FI about any erroneous transaction, provide the wrong recipient's FI with a response.
- c. The timelines specified above assume that the case is straightforward. FIs are to use their best efforts to respond within the timelines specified above. The FIs may take longer to convey instructions in complex cases such as where any party to the transaction is

resident overseas or where the FIs have not received sufficient information from the account holder to convey instructions within the specified timeline. For the avoidance of doubt, the FIs are not expected to resolve each erroneous transaction claim but to facilitate effective communication between the account holder and the recipient with the aim to improve the account holder's chances of recovering the payment amount sent through the erroneous transaction.

3. Account holder or recipient to provide information on erroneous transaction

- a. For the purposes of assisting the account holder's FI to recover sums sent in error, the account holder should provide his FI with any of the following information as requested by the FI:
 - i. all the information set out in paragraph 3.9(a) except limbs (v), (vi) and (vii);
 - ii. the recipient's unique identifier, including account number, identification number, name or other credentials entered by the account user; and
 - iii. the date, time, amount and purpose of the erroneous transaction insofar as such information is known to the account user.
- b. For the purposes of assisting the recipient's FI to return sums sent in error, the recipient should provide his FI with any of the following information as requested by the FI:
 - i. the protected account(s) to which the erroneous transactions have been made;
 - ii. the date, time and amount of the erroneous transaction insofar as such information is known to the recipient; and
 - iii. any other relevant information about the erroneous transaction that is known to the recipient.

7. DISPUTE RESOLUTION PROCESS FOR HANDLING ANY DISPUTED INVESTIGATION

This paragraph applies when the account holder does not agree with the investigation outcome of the relevant claim, set out in paragraphs 4.13 to 4.14 above, by the Bank ("disputed investigation").

1. Bank to have in place a dispute resolution process

- a. The Bank should have a dispute resolution process for handling any disputed investigation.

2. Bank to provide channels for account holders to notify the Bank

- a. The Bank should provide account holders of protected accounts with a channel to raise the disputed investigation. The channel could take the form of, but not limited to:

- i. a manned phone hotline or physical branch;
- ii. the Bank's mobile application; or
- iii. the customer support chat function on the Bank's website.

3. Reasonable request for evidence by the Bank to facilitate investigations

- a. The Bank may request information from the account user such as records of correspondences (e.g. email or SMS logs from the telecommunication service provider if the account user is able to obtain it, or screenshots of the correspondence or SMS received on the account user's mobile phone) to facilitate the investigation of the disputed investigation.

4. Bank to promptly assess and investigate the disputed investigation

- a. The Bank should assess and complete an investigation of any disputed investigation raised by an account holder within 21 business days or where there are exceptional circumstances, within 45 business days of receipt of the disputed investigation. Exceptional circumstances may include delays caused by other external parties involved in resolving the dispute.
- b. The Bank should first assess if there are any grounds for further investigation to be made on the disputed investigation.
 - i. Where the Bank has assessed that there are no grounds for further investigation to be carried out on the disputed investigation, the Bank should communicate the reasons why no further investigation would be carried out to the account holder in accordance with paragraph 7.4(c).
 - ii. Where the Bank has assessed that there are grounds for further investigation to be carried out on the disputed investigation, the Bank should complete the investigation and inform the account holder of the investigation outcome in accordance with paragraph 7.4(c).
 - iii. Where the Bank needs to extend the investigation period beyond 21 business days due to exceptional circumstances, the Bank should inform the account holder of the need for additional time to complete its investigation.
- c. The Bank should within the time periods set out in paragraph 7.4 give each account holder that notified the Bank of the disputed investigation, a written or oral report of the outcome of the assessment and investigation of the disputed investigation that includes the following information:
 - i. the outcome of the assessment and investigation of the disputed investigation;
 - ii. the reasons for the outcome, including the assessment of the account holder's liability based on the relevant considerations under paragraph 5. This could include how the account user may have been reckless or have not complied with any duty set out in paragraph 3;

- iii. instructions for the account holder to pursue the matter further if the account holder does not agree with the assessment and investigation outcome, including the availability of dispute resolution by FIDReC;
 - iv. FIDReC's contact information: For complainants: info@fidrec.com.sg; For feedback: feedback@fidrec.com.sg; Address: 36 Robinson Road, #15-01 City House Singapore 068877; Tel: (65) 6327 8878; Fax: (65) 6327 8488 / (65) 6327 1089.
- d. Paragraphs 7.4(a) and 7.4(b) do not apply if the disputed investigation relates to a transaction performed on a credit card, charge card or debit card issued by the Bank, and the Bank exercises its rights to resolve the dispute under the rules of the card scheme.

8. CHARGES RELATING TO TRANSACTIONS UNDER DISPUTE

1. Bank to withhold and/or waive charges relating to transactions under dispute

- a. Where an account holder reports a suspected unauthorised transaction ("disputed transaction"), the Bank should withhold and/or waive the requirement for the account holder to settle the outstanding amount of the disputed transaction and the charges (e.g. late payment fee, fall-below-balance service fee, telegraphic transfer commission, fees and charges facilitating the movement of funds during the Bank's investigation and charges not within the Bank's control such as agent fee and cable charge) directly relating to the disputed transaction until the Bank completes its investigation of the disputed transaction.
- b. Where the Bank has assessed that the disputed transaction is an authorised transaction or an unauthorised transaction for which the account holder is liable, and the account holder does not agree with the assessment, the Bank should withhold and/or waive the requirement for the account holder to settle the outstanding amount of that transaction and the charges directly relating to that transaction during the following periods:
 - i. from the date the Bank completes its investigation up to 30 calendar days after the Bank informs the account holder of the investigation outcome. This is in recognition that the account holder may not agree with the Bank's assessment of the account holder's liability of the unauthorised transaction in accordance with paragraph 5 and intends to commence dispute resolution with FIDReC.
 - ii. from the date when the Bank is aware that the consumer has commenced dispute resolution with FIDReC up to the completion of mediation and/or adjudication by FIDReC or when the case is closed by FIDReC due to prolonged inactivity.

2. Bank to withhold the reporting of the non-payment of disputed transactions to licensed credit bureaus

- a. Where the disputed transaction is made using credit cards or other unsecured credit facilities, the Bank should ensure that the account holder's credit records with licensed credit bureaus are not adversely affected due to the disputed transaction:
 - i. until the Bank completes its investigation of the disputed transaction; or
 - ii. in the event where the non-payment of the disputed transaction had already been reported to licensed credit bureaus, after the Bank completes its investigation of the disputed transaction and the account holder was found to be not liable for the disputed transaction.
- b. Where the Bank has assessed that the disputed transaction is an authorised transaction or an unauthorised transaction for which the account holder is liable, and the account holder does not agree with the assessment, and the transaction is made using credit cards or other unsecured credit facilities, the Bank should ensure that the account holder's credit records with licensed credit bureaus are not adversely affected due to that transaction during the following periods:
 - i. from the date the Bank completes its investigation up to 30 calendar days after the Bank informs the account holder of the investigation outcome; and
 - ii. in the event where the consumer has commenced dispute resolution with FIDReC, after the completion of mediation and/or adjudication by FIDReC or when the case is closed by FIDReC due to prolonged inactivity.
- c. After the time periods set out in paragraphs 8.1 and 8.2, the Bank may resume the reporting of any unpaid outstanding amounts for the disputed transaction to licensed credit bureaus if the account holder has not repaid the amount due 7 calendar days from the date of the Bank's request.

3. Bank to disclose charges relating to recovery of unauthorised transactions

- a. Where there are any charges or costs relating to the recovery of the unauthorised transaction amount (such as agent fee, arbitration charge, foreign exchange rate differences, professional fee) to be borne by the account holder, the Bank should disclose such charges to the account holder.

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

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.

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

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.sbisg.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