You have an important role to play to ensure that you and your account(s) are protected while banking with us electronically. Here are some useful tips:

Notice on Customer Duties

The E-Payments User Protection Guidelines (the “Guidelines”) issued by the Monetary Authority of Singapore (“MAS”) set out the expectations of MAS of any responsible financial institution that issues or operates a protected account. The Guidelines also cover duties of account holders and account users of protected accounts, and provide guidance on the liability for losses arising from unauthorised and erroneous transactions.

Some important definitions in the Guidelines include:

(1) a "payment account" as:

(a) any account, or any device or facility (whether in physical or electronic form), that —

- (i) is held in the name, or associated with the unique identifier, of any person, and is used by that person for the initiation of a payment order or the execution of a payment transaction, or both; or
- (ii) is held in the names, or associated with the unique identifiers, of 2 or more persons, and is used by any of those persons for the initiation of a payment order or the execution of a payment transaction, or both; and

(b) includes a bank account, debit card, credit card or charge card.

(2) a “payment transaction” as 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;

(3) a “protected account” as 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.

(4) an "unauthorised transaction" (in relation to any protected account) as 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 biometrics identities on their devices. The account holder is deemed to have consented to the use of his account by this person.

(5) the “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.

Note: For Citi Private Bank, this transaction notification threshold is maintained at $0, which means that transaction alerts will be sent for all payment transactions (regardless of the dollar value of the payment transaction).

(6) the “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 responsible FI 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.

Note: For Citi Private Bank, the option to perform (b) increasing transaction limits for outgoing payment transactions is not available on Citi Private Bank In View App and website

In accordance with the Guidelines, Citi Private Bank would like our customers and account users of protected accounts to take note of (a) their duties set out in section 3 of the Guidelines, and (b) the duties of any responsible financial institution that issues or operates a protected account set out in section 4 (excluding paragraph 4.3 of the Guidelines). You should note that 4.4, 4.7, 4.8, 4.9, 4.10, 4.14, 4.15, 4.19, 4.20, 4.21 of the Guidelines are enhanced duties that are applicable to retail customer segments. Citi Private Bank will nonetheless ensure that systems and controls would still meet the spirit of the additional duties. Please carefully review the Guidelines here.

We would like to draw your attention to section 3 of the Guidelines which provides for the customer/account user's duties. Some of these duties are highlighted below. These are not intended to be exhaustive and you should refer to the Guidelines (link above) for further details on customer/account user's duties.

(a) **Provide contact information, opt to receive all outgoing transaction notifications and monitor notifications**. It is your responsibility to provide us with complete and accurate contact information in order for us to send you notification alerts for transactions, activation of digital security token and the conduct of high-risk activities. You are also responsible to (i) enable notification alerts via SMS, email or in-app/push notification on any device (used to receive notification alerts from Citi Private Bank); (ii) opt to receive notification alerts for all outgoing transactions made from your protected account, activation of digital security token and the conduct of high-risk activities made from your protected account, and (iii) monitor the notification alerts sent to you or the designated account contact. (For this reason, Citi Private Bank will assume that you will monitor such notification alerts without further reminders or repeat notifications.)

If you wish to select/change preferences to your notification alerts, simply login to https://www.privatebank.citibank.com with your User ID & Password and select 'Notifications' under 'Settings'.

(b) **Protect your access codes**. You should protect the access codes that you use to authenticate any payment transaction or your identity (e.g. your password or OTP) and not voluntarily disclose these to any third party, including the staff of Citi Private Bank. You should not keep a record of any access code in a way that allows any third party to easily misuse the access code.

(c) **Secure access to your protected account**. You should only download our Citi Private Bank In View App from official sources. You should ensure that you have strong passwords and install and maintain your device with the latest anti-virus software. You should also ensure to update your device's browser to the latest version available and patch your device's operating systems with regular security updates provided by the operating system provider. You should not root or jailbreak your device nor 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.

(d) **Notify all account users on security instructions or advice.** As an account holder, you should notify all account users of the security instructions or advice provided by Citi Private Bank. As an account user, you should also follow security instructions or advice provided by Citi Private Bank to the account holder.

(e) **Read content sent with access codes**. You should read the content of the messages containing the access codes and verify that the stated recipient or activity is intended prior to completing transactions or high-risk activities.

(f) **Obtain Citi Private Bank's website address and phone numbers from official sources and contact Citi Private Bank using contact details from official sources.** You should refer to official sources (for example the Citi Private Bank In View App or your Citi Private Bank representative) to obtain our website address and phone numbers.

(g) **You should not click on links or scan QR codes.** You should not click on links or scan QR codes purportedly sent by Citi Private Bank unless you are expecting to receive information on Citi Private Bank products and services via these links or QR codes. Citi Private Bank will not send you links or QR codes which directly result you in providing us any access code or to make a payment transaction or high-risk activity.

(h) **You should understand the risks and implications of performing high-risk activities.** Before performing any high-risk activities, you should read Citi Private Bank's risk warning message and ensure you understand the risks and implications of proceeding. If you do not understand the risks and implications of proceeding with the high-risk activities, you should access the Citi Private Bank website for more information or contact Global Services & Support or your Citi Private Bank representative prior to performing these activities. By proceeding, you are deemed to have understood the risks and implications as presented by Citi Private Bank.

(i) **You should report unauthorised activities on your protected account and provide the required information to Citi Private Bank.** You should report any unauthorised activity on your protected account to Citi Private Bank as soon as practicable, and no later than 30 calendar days after receipt of any notification alert for any unauthorised activity. In connection with your report, you should provide us with any of the information as set out in section 3.18 of the Guidelines upon our request within a reasonable time.

(j) If you are notified of any unauthorized transactions and have reason to believe that your account has been compromised, please contact Global Services & Support or your Citi Private Bank representative as soon as practicable, to block further mobile and online access to your protected account.

(k) **You should make a police report if you suspect you are a victim of scam or fraud.** Citi Private Bank requires you to provide a police report to facilitate our claims investigation process. You should fully cooperate with the Police and provide evidence (such as furnishing your mobile device to the Police for forensics investigation).

We would like to draw your attention to section 4 of the Guidelines which provides for the duties of any responsible financial institution that issues or operates a protected account. Some of these duties are highlighted below. These are not intended to be exhaustive and you should refer to the Guidelines (link above) for further details.

(a) Citi Private Bank will not send phone numbers via SMS to you unless you are expecting to receive such an SMS from Citi Private Bank.
(b) Citi Private Bank will ensure that Citi Private Bank's website address and contact details provided from official sources (for example the Citi Private Bank In View App or your Citi Private Bank representative) are up to date.
(c) While Citi Private Bank should make available to you the option to receive transaction notification alerts for all outgoing payment transactions made from your protected account, if you instruct or have instructed Citi Private Bank otherwise, notification alerts for outgoing transactions will be provided in accordance with your instructions.
(d) Citi Private Bank should make available on its website or mobile application information on how you can adjust the transaction notification settings. Citi Private Bank should explain how your liability under Section 5 of the Guidelines may be affected by your transaction notification preferences and how any relevant claim by you (as defined in paragraph 4.22 of the Guidelines) will be resolved.
(e) In order for you to identify the payment recipient, information that allows you to identify the protected account, the recipient, the intended transaction amount (including currency) and a warning to remind you not to reveal the access code to anyone, should be provided to your accompanying access codes (such as one-time passwords sent via SMS or equivalent push notifications via mobile application) in the same message sent to you.
(f) Where a transaction is effected by way of internet banking, any mobile phone application or device arranged for by Citi Private Bank for payment transactions, an onscreen opportunity will be provided for you to confirm the payment transaction, recipient credentials and a warning to check the information before you execute any authorized payment transaction.
(g) Citi Private Bank may require you to furnish a police report in respect of an unauthorised transaction claim before the claims resolution process is commenced. In this regard, if you request for information on the procedure to file a police report, Citi Private Bank will provide such information to you.
(h) Citi Private Bank may request you to provide the information set out at paragraph 3.18 of the Guidelines. Upon enquiry from you, Citi Private Bank will provide to you relevant information that Citi Private Bank has of all unauthorised transactions which were initiated or executed from a protected account, including transaction dates, transaction time stamps and parties to the transaction.
(i) Citi Private Bank should complete an investigation of any relevant claim within 21 business days for straightforward cases or 45 business days for complex cases. Within the aforementioned time periods, a written or oral report of the investigation outcome and an assessment of liability in accordance with Section 5 of the Guidelines should be provided and Citi Private Bank should seek acknowledgement from you of the investigation report.

(j) If you do not agree with Citi Private Bank's assessment of liability, or where Citi Private Bank has assessed that the claim falls outside of Section 5 of the Guidelines, either party may commence other forms of dispute resolution, including mediation at the Financial Industry Disputes Resolution Centre Ltd.
(k) Citi Private Bank should credit your protected account with the total loss arising from any unauthorised transaction as soon as Citi Private Bank has completed its investigation and assessed that you are not liable for any loss arising from the unauthorised transaction. This arrangement, as well as the timeline for completing the investigation as set out at (i) above, should be disclosed to you at the time that you report the unauthorised transaction to Citi Private Bank.
(l) Where applicable, the delivery of key services and alternatives will continue during a scheduled downtime, and such downtime should not be performed during periods where high volume or transactions are expected.

Liability Framework for Unauthorised Transactions under the Guidelines

The below mentions the Guidelines set out in section 5, a liability framework relating to unauthorized transactions effected on a protected account.

An account user would be responsible for actual loss arising from an unauthorised transaction if such account user's recklessness was the primary cause of loss. Recklessness would include the situation where the account user deliberately did not comply with the duties set out in section 3 of the Guidelines. It is therefore important for you to read and understand your duties under section 3 of the Guidelines to understand how any deliberate non-compliance with your duties would affect how the liability framework in section 5 of the Guidelines would be applied and how any claim by you in relation to an unauthorised transaction would be resolved.

As set out in the Guidelines, 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 responsible FI;
(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 responsible FI has:
  • specifically instructed the account holder not to do so, and
  • warned the account holder of the consequences of doing so.

Please note that the disabling of transaction notifications would restrict your ability to be made aware of potential unauthorised transactions from your protected account and could affect your liability under section 5.

Further, Customers should note that the Guidelines provide that "where any account user knew of and consent to a transaction ("authorised transaction"), such a transaction is not an unauthorised transaction, notwithstanding that the account holder may not have consent to the transaction."

The information set out below has been distilled from section 5 of the Guidelines and is not intended to be exhaustive. Customers are advised to read the Guidelines for full details.

Scenario (1): Customer is liable for actual loss

The customer will be liable for the actual loss arising from an unauthorized transaction on a protected account if the customer/account user's recklessness was the primary cause of the loss. Recklessness would include the situation where any account user deliberately did not comply with section 3 of the Guidelines. Please also refer to the above examples of conduct that constitute recklessness.

Scenario (2): Customer is not liable for any loss

The customer is not liable for any loss arising from an unauthorized transaction if the loss arises from any action or omission by Citi Private Bank and does not arise from any failure by any account user to comply with any duty in section 3 of the Guidelines.
Any action or omission by Citi Private Bank includes the following:

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

(b) non-compliance by Citi Private Bank or its employee with any requirement imposed by MAS on Citi Private Bank in respect of its provision of any financial service; and
(c) non-compliance by Citi Private Bank with any duty set out in section 4 (excluding paragraph 4.3) of the Guidelines. You should note that 4.4, 4.7, 4.8, 4.9, 4.10, 4.14, 4.15, 4.19, 4.20, 4.21 of the Guidelines are enhanced duties that are applicable to retail customer segments. Citi Private Bank will nonetheless ensure that systems and controls would still meet the spirit of the additional duties.

Scenario (3): Loss resulting from any action or omission of any independent third party

The customer is not liable for the first S$1,000 of loss arising from an unauthorised transaction, if the loss arises from any action or omission by any third party not referred to in scenario (2) above, and does not arise from any failure by any account user to comply with any duty in section 3 of the Guidelines.

Last updated: 16 December 2024

Other Advisory

Always make sure that you have entered your User ID and Password and other confidential information in the legitimate Citi Private Bank Website by entering Citi Private Bank's website address https://www.privatebank.citibank.com directly onto your Web browser.