1. What are your responsibilities as an account holder?

S/N	Responsibility	Details

1	**Contact information, option to receive and transaction notifications**	• You must provide us with the contact details we need in order for us to send you transaction notifications, as set out in this Policy. Where the protected account you have with us is a joint account, all account holders must jointly give instructions to us on which account holder(s) should receive transaction notifications.
		• It is your responsibility and the responsibility of any account user to:
		  ○ enable notifications on any device used to receive transaction notifications;
		  ○ opt out or modify how you receive transaction alerts; and
		  ○ monitor the transaction notifications sent to you.
		• You must inform us immediately of any change to your contact details including the following:
		  ○ mailing address;
		  ○ Singapore registered mobile phone number; and
		  ○ email address.

2	**Protection of Access Codes**	• You must protect any access code that we provide to you to authenticate any payment transaction. The following list (not exhaustive) are examples of access codes that we may send to you or the account user:
		  ○ Personal identification number, password or code;
		  ○ Internet banking authentication code;
		  ○ Telephone banking authentication code;
		  ○ Code generated by an authentication device e.g. token; and
		  ○ Code sent by us through text messages such as SMS.
		• You and any account user must not to do any of the following:
		  ○ Voluntarily disclose any access code to any third party, including any of our staff.
		  ○ Disclose the access code in a recognisable way on any payment account, authentication device or any container for the payment account.
		  ○ Keep a record of any access code in a way that allows any third party to easily misuse the access code.
		• You must always keep the record of an access code in a secure electronic or physical location accessible or known only to the account user which is a place where the record is unlikely to be found by a third party

3	**Protection of Account**	• You should read the content of the messages containing any access codes and verify that the stated recipient or activity is intended prior to completing any transaction.
		• You should refer to official sources to obtain our website address and phone number. Examples of official sources include the MAS Financial Institutions Directory, our mobile application and the back of cards (e.g. credit card, debit card or charge card), which may change from time to time.
		• You should not click on links or scan Quick Response codes (“QR codes”) purportedly sent by us unless you are expecting to receive information on products and services via these links or QR codes from us.
		• You should read the risk warning messages sent by us before proceeding to confirm the performance of high-risk activities. High-risk activities include, but are not limited to:
		  ○ adding of payees;
		  ○ increasing the transaction limits for outgoing payment transactions;
		  ○ disabling transaction notifications from us; and
		  ○ changing your contact information including mobile number, email address and mailing address.

2. What are our responsibilities as a bank?

S/N	Responsibility	Details
1	**Cooling off period for high-risk activities**	We will impose a cooling off period of at least 12 hours where high-risk activities cannot be performed, when a digital security token is activated on a device.
2	**Notifications for high-risk activities**	When we send you notifications for performance of high-risk activities or activation of your digital security token we will: a) send the notifications to every account contact selected by you; b) ensure that the notifications will be sent to you on a real time basis; c) send the notifications to you either by SMS or email (even if you have already received a push notification via any Maybank app); d) ensure that the notifications contain relevant information on the performance of the high-risk activities or activation of your digital token, e.g. information on payee added, new transaction limits or a change in contact details; and e) include in the notifications a reminder to you to contact us if you did not perform the high-risk activity or activate the digital security token.
3	**Transaction Notifications**	• Provided that you have fulfilled your obligations stated in this Policy and the Terms and Conditions, we will send you notifications for all payments you make through electronic means. These include fund transfers, debit/credit card transactions and bill payments. At this point in time, we will not send you notifications for incoming transactions unless you opt-in to receive such notifications. When we send you a transaction notification we will: a) send the transaction notifications to every account contact selected by you; b) ensure that transaction notifications will be sent to you on a real time basis; c) send transaction notifications to you either by SMS or email (even if you have already received a push notification via any Maybank app); d) ensure that transaction notifications contain the following information: i. Information that allows you to identify the protected account such as the account number; ii. Information that allows you to identify the recipient whether by name or by other credentials such as the recipient's account number; iii. Information that allows us to later identify you, the protected account, and the recipient account; iv. Transaction amount; v. Transaction time and date; vi. Transaction type; and vii. 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. We will ensure that the information provided still allows you to identify the transaction as being an authorised or unauthorised transaction.
4	**We will inform you of the details of any recipient**	Where transactions are made by way of internet banking, any mobile phone application or device arranged for payment transactions, including a payment kiosk, we will provide an onscreen opportunity for the person who is making the transaction to confirm the payment transaction and recipient credentials before we execute any authorized payment transaction. The onscreen opportunity will contain the following information: a) information that allow the account user to identify protected account to be debited;

S/N	Responsibility	Details
		b) the transaction amount; and c) the credentials of the intended recipient (e.g. account number, name registered for receiving payments, identification number and phone number).

3. How do I protect myself against losses from erroneous and/or unauthorised transactions?

As an account or joint account holder, you are recommended to:

- Provide complete, accurate and updated contact information (*Login to Maybank Online Banking → Select Settings → Under Personal → Select Personal Information or Contact Details or Address → Click on the pencil icon next to the specific detail you wish to update)*
- Enable and/or modify transaction notification alerts (*Login to Maybank Online Banking → Select Settings → Under Security → Select E-Payment Alerts)*
- Monitor the transaction notification alerts sent by the Bank
- Safeguard your account and internet banking credentials securely and do not share with anyone
- Check the details carefully before proceeding to confirm the transaction

4. Am I protected against losses from scam or fraud?

You are liable for actual loss arising from an unauthorised transaction where any account user's recklessness was the primary cause of the loss. Recklessness would include the situation where the account user deliberately did not comply with their obligations under E-Payment Policy. The actual loss that you are liable for is capped at any applicable transaction limit or daily payment limit that we have agreed to.

For the avoidance of doubt, where any account user knew of and consented to a transaction, such transactions are not considered to be an unauthorised transaction notwithstanding that the account holder may not have consented to the transaction. The account holder of the protected account is liable for all authorised transactions up to any applicable transaction limit or daily payment limited that we have agreed to.

5. What should I take note of before making an E-Payment transaction?

Protect the access to your account by:

- Downloading our mobile application(s) only from official sources
- Updating your device's web browser to the latest version available
- Updating your device's operating systems with regular security updates provided by the operating system provider
- Installing and maintaining latest anti-virus software on your device(s), where applicable
- Using strong and unique passwords such as a mixture of letters, numbers and symbols or strong authentication methods such as facial recognition or fingerprint authentication methods
- Not rooting or jailbreaking the device
- Not downloading or installing applications from third-party websites outside official sources
- Following the security instructions and guidelines shared by the Bank

Please note that the above list is the minimum you should do to protect your protected account with us. The list is not exhaustive and we may change or supplement the list from time to time. You must ensure that you, as an account holder, inform all the authorised users of the security instructions or advice provided by us to you.

6. What should I do if I detect erroneous and/or unauthorised transactions?

Inform us immediately:

Local	: 1800-MAYBANK (1800-629 2265)
Overseas	: (65) 6533 5229

If you are unable to report to the Bank as soon as you receive the transaction notification alert, you should provide the Bank with reasons for the delay when asked. In any event, you must report any unauthorised transactions to us no later than 30 calendar days after you receive any transaction notification alert for any unauthorised transaction.

7. What information do I have to provide when reporting to the Bank?

Provide the Bank with information on:

- The protected account that is affected, including your affected accounts with other financial institutions if any;
- The account holder identification information;
- The type of authentication device, access code and device that is used to perform the payment transaction;
- The name or identity of any account user for the protected account that was used;
- Details on whether or not the protected account's authentication device or access code was lost, stolen and misused and if so, the:
  - Date and time of loss or misuse;
  - Date and time that the loss or misuse was reported to us; and
  - Date, time and method that the loss or misuse was reported to the police
- If access code is applicable to the protected account:
  - How the account holder/user recorded the access code; and
  - Whether the account holder/user had disclosed the access code to anyone
- Any other information about the unauthorised transaction that we may require.

You will receive an acknowledgement of the unauthorised report from us either via email or via SMS.

In addition to informing us, you should also make a police report as soon as practicable for the unauthorised transaction in order to facilitate the investigation process, or if you suspect that you are a victim of scam or fraud.

8. What can I do to protect my funds from scams and unauthorised transfers or withdrawal?

a) Money Lock

Money Lock is an added layer of protection designed to protect the funds in your current or savings account(s) from the reach of scammers.

You may lock funds in excess of what was needed for regular or budgeted expenses. Lock funds can be done via Maybank2u Online Banking, Maybank2u SG mobile app, at selected ATMs or at any Maybank Singapore branches. Once the funds are locked, you will not be able to access them. They will be kept safe until you are ready to unlock the funds.

b) Kill Switch

In the event of emergency, such as scam or fraud, you can conveniently suspend your digital banking access via Kill Switch on Maybank2u SG app or Maybank2u Online Banking.

Suspension of digital banking access is immediate. Once your digital banking access is suspended, you will no longer be able to log in to Maybank2u online or mobile banking.

c) To avoid falling for online banking scams, you must:
   a. Always ensure contact details are updated
   b. Set transaction alerts to stay informed of any banking activities
   c. Never transfer money to people you do not know;
   d. Never click on links provided in unsolicited SMSes or emails;
   e. Verify unsolicited SMSes or emails received by calling the bank directly on the hotline listed on its official website;
   f. Always check that you are at the bank's official website before making any transaction or transact through the bank's official mobile application;
   g. Never divulge internet banking credentials or passwords to anyone;
   h. Secure your device with a strong password, PIN or a relevant mechanism to prevent unauthorised use; *TIP: A strong password is one that is difficult to guess and contains a mix of letters, numbers or symbols. You can use this on top of your device's biometric security feature (if available).*
   i. Use a different PIN or password for web-based services such as email, online shopping or subscription services; and
   j. Monitor transaction notifications closely so that any unauthorised payments are reported as soon as possible to increase the chances of recovery.