

ANEXT BANK PTE. LTD.
E-Payments User Protection Guidelines

Singapore has widely adopted e-payments and in a bid to strengthen the security and simplicity of such, the Monetary Authority of Singapore (MAS) issued the E-Payments User Protection Guidelines (“Guidelines”).

While financial institutions could be held responsible for individuals' and sole proprietors' losses arising from unauthorised and erroneous e-payment transactions, account holders and operators are also responsible for adopting safe and secure banking practices.

Please read these frequently asked questions on the Guidelines and click [here](#) for recommended cyber security practices.

1. What is a protected account?

A protected account is a payment account that:

- is held by one or more individuals and/or sole proprietors, including those held jointly by multiple account holders;
- is a credit facility or can hold a balance of more than SGD 1,000 (or its equivalent amount in another currency) at any one time; and
- can be used for receiving, transferring or withdrawing money via electronic means.

These Guidelines would be applicable to you if you are a sole proprietor holding an account with ANEXT Bank.

2. What e-payments are covered by the Guidelines?

All payments initiated from protected accounts through electronic means (other than payments you initiated because of a scam or fraud), and funds received to protected accounts through electronic means, such as online payments and transfers, are covered by the Guidelines.

3. How do the Guidelines protect me?

We will provide you with notification alerts, and a reporting channel, so that you may be alerted of unauthorised transactions and report them should they happen. We will investigate all claims of unauthorised transactions, with the aim of achieving a fair and reasonable resolution.

The Guidelines do not apply to transactions which you initiated because of a scam or fraud. If you suspect or have reason to believe that you are a victim of a scam or fraud, you are advised to lodge a police report for police investigations.

4. What are my duties as an account holder or account operator?

The Guidelines set out your duties as a protected account holder or account operator to adopt good security practices. These include:

- a. Ensuring that your contact information (e.g., Mobile phone number and email address) are complete and accurate at all times so that we can send you notification alerts.
- b. Enabling notification alerts on your device(s) used to receive such alerts.
- c. Monitoring your notification alerts and reporting to us as soon as possible if you become aware of any unauthorised or erroneous transaction(s).
- d. Safeguarding your access credentials to your protected account (such as your password, security code, PIN, OTP or any other credentials used to authenticate your identity and/or initiate or execute any payment transaction) by **not** performing any of the following:
 - i. Voluntarily disclosing any access credentials to any third party (including the Bank's employees);
 - ii. Disclosing the access credentials in a recognisable way on any payment account, authentication device, or any container for the payment account; or
 - iii. Keeping a record of any access credentials in a way that allows any third party to easily misuse the access credentials.
- e. Making reasonable efforts to secure any record of any access credentials by keeping the record in a secure electronic or physical location accessible or known only to the account operator and keeping the record in a place where the record is unlikely to be found by a third party.
- f. Practicing good digital security hygiene by ensuring that:
 - i. Your device's browser is updated to the latest version;
 - ii. Your device's operating system is patched on a regular basis with security updates provided by your device's operating system provider;
 - iii. Your device has the latest anti-virus and anti-malware software installed and is regularly maintained through updates;
 - iv. Your password protection is strong through a mixture of alphabets and numbers with a minimum of 12 characters (20 characters max). Passwords should not be repetitive and easy to guess;
 - v. You do not root or jailbreak the devices used;
 - vi. You do 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; and

- vii. You only download and use our Mobile Banking App from the official app stores (Apple App Store, Google Play Store or Huawei AppGallery).
- g. (where applicable) Informing all of your protected account operators of the security instructions or advice provided by us and where possible, following the security instructions or advice provided by us.
- h. Reading and verifying the content sent with access codes before completing payment transactions or high-risk activities.
- i. Only referring to official sources (i.e., MAS Financial Institutions Directory) to obtain the contact details (i.e., website address and phone number) of the Bank.
- j. Not clicking on links or scan QR codes purportedly sent by the Bank unless the links are to solely provide information to you such as regulatory requirements (i.e., Terms and conditions), product description, steps to execute a transaction, fact sheet for investment products.
- k. Understanding the risk and implications of performing high-risk activities (see below paragraphs 7 and 8).
- l. Activating the self-service feature to promptly block further mobile and online access to your protected account (see [here](#) under FAQs -> Security).
- m. Reporting any unauthorised or erroneous transaction(s) to us as soon as possible upon your receipt of any notification alerts or otherwise becoming aware; and lodging a police report if we require such a report to be made to facilitate our claims investigation process.

5. Why do I need to activate notification alerts on my device?

The notification alerts safeguard you against unauthorised and erroneous transactions. They are to alert you of all transactions on a timely basis so that you may report any unauthorised or erroneous transactions to us as soon as possible.

6. What type of notification alerts will I receive?

You will receive notification alerts for (i) transactions such as all outgoing payments initiated from your protected account through electronic means, and where funds are received to your protected account through electronic means, such as online payments and transfers, (ii) activation of your digital security token and (iii) whenever a high-risk activity is conducted.

7. What is considered as a high-risk activity?

A high-risk activity includes, but is not limited to:

- Adding of payees to the account holder's payment profile;
- Change in the account holder's contact information including mobile number, email address and mailing address;
- Increasing the transaction limits for outgoing payment transactions from a payment account; and
- Disabling transaction notifications that will be sent upon completion of a payment transaction.

8. What are the risks and implications of performing high-risk activities?

High-risk activity	Risks and implications (non-exhaustive)
Adding of payees to the account holder's payment profile	Account operators will be able to make outgoing fund transfers to the new payees. If this was not authorised or done erroneously, this may lead to unauthorised or erroneous outgoing fund transfers.
Change in the account holder's contact information including mobile number, email address and mailing address	Account-related notifications and/or communications will be sent to the updated mobile number, email address and mailing address. If this was not authorised or done erroneously, you will not receive account-related notifications and/or communications from us when there is account activity.
Increasing the transaction limits for outgoing payment transactions	Account operators will be able to make outgoing fund transfers up to the new transaction limit. If the increase is not authorised or done erroneously, this may lead to unauthorised or erroneous outgoing fund transfers above the original transaction limit.
Disabling transaction notifications that will be sent upon completion of a payment transaction	Transaction notifications will not be sent after a payment transaction is completed. If this was not authorised or done erroneously, you will not receive notifications from us when such transactions are made.

9. What is the difference between unauthorised transactions and erroneous transactions and what should I do and expect if I become aware of such transactions?

	Unauthorised Transaction	Erroneous Transaction
Definition	Any payment transaction initiated by	Any payment transaction initiated

	<p>any person without the actual or implied knowledge and implied or express consent of the account holder or operator of a protected account. This includes “seemingly authorised transactions”.</p> <p>“seemingly authorised transactions” in relation to any protected account, means any payment transaction which fulfils limbs (a) to (d) immediately below:</p> <p>(a) perpetrated through the impersonation of a legitimate business or government entity, e.g., FIs, non-banks and government agencies (“impersonated entity”);</p> <p>(b) the scammer, pretending to be the impersonated entity, uses a digital messaging platform (e.g., SMS, email, WhatsApp, social media platforms) to obtain the account operator’s account credentials (this includes access codes and user IDs);</p> <p>(c) The account operator enters his account credentials on a fabricated digital platform (e.g., website, application) (“fraudulently obtained credentials”); and</p> <p>(d) The fraudulently obtained credentials are used to perform transactions that the account operator did not intend to be performed.</p> <p>The following are examples of payment transactions that do not fall within the scope of unauthorised transactions:</p> <p>(a) The account holder or operator</p>	<p>from a protected account such that money has been placed with or transferred to the wrong recipient.</p>
--	---	---

	<p>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);</p> <p>(b) The transaction was performed by a person as a result of the account holder or operator sharing access and usage of their devices with the person, or storing the person's biometrics identities on their devices. The account holder or operator is deemed to have consented to the use of his account by this person.</p> <p>For the avoidance of doubt, where any account operator knew of and consented to a transaction, 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 operator acts fraudulently to defraud any account holder or us.</p>	
(1) How can I report to ANEXT Bank?	<p>(a) Call Business Support at 1800 268 8888 or (65) 6813 3688 from 9:00am - 6:00pm, Monday to Friday except Public Holidays.</p> <p>(b) Submit your report via the 'Get Help -> Contact Us' form on our official website</p>	
(2) What should I prepare?	<p>We will require the following information from you:</p> <ul style="list-style-type: none"> • The bank account affected, including any other affected accounts with other FIs; • Your identification information; • The type of device and access 	<p>We will require the following information from you:</p> <ul style="list-style-type: none"> • The bank account affected, including any other affected accounts with other FIs; • Your identification information; • The type of device and access

	<p>credentials used to perform the unauthorised transaction;</p> <ul style="list-style-type: none"> • The name or identity of any account operator; • Whether the account number, device or access credentials was lost, stolen or misused and if so, <ul style="list-style-type: none"> • the date and time of the loss, theft or misuse, • the date and time that the loss, theft or misuse, was reported to us, and • the date, time and method that the loss, theft or misuse, was reported to the police; and • (where any access credentials are applicable to the account) (i) how you as the account holder or any account operator recorded the access credentials, and (ii) whether you as the account holder or any account operator had disclosed the access credentials to anyone, and (iii) any other information about the unauthorised transaction that is known to the account holder or any account operator (such as a description of the scam incident; whether the account holder received any transaction notifications / OTPs sent by us and where applicable, a confirmation from telco operators to verify the receipt status only if the account holder is able to obtain it; any suspected compromised applications in the account operator's device) 	<p>credentials used to perform the erroneous transaction;</p> <ul style="list-style-type: none"> • The name or identity of any account operator; • The wrong recipient's unique identifier, including account number, identification number, name or other credentials entered by the account holder or any account operator; and • The date, time, amount and purpose of the erroneous transaction to the extent as such information is known to the account holder or any account operator.
--	---	--

	Where required, you may need to lodge a police report to facilitate our investigations, and furnish the police report to us within 3 calendar days from our request.	
(3) What can I expect after reporting?	<p>Any person who makes a report through the reporting channel as above will receive a written acknowledgement of his/her report through SMS or email.</p> <p>After receiving information required to facilitate our investigations, we will endeavour to complete our investigation of any relevant claim within 21 business days for straightforward cases or 45 business days for complicated cases.</p> <p>Complex cases may include cases where any party to the unauthorised transaction is resident overseas or where we have not received sufficient information from you to complete our investigations.</p> <p>We will update you with a written or oral report of the outcome of our investigation as well as our assessment of your liability, if any.</p> <p>If it has been assessed that you are not liable for any loss from the unauthorised transaction, we will credit your account as soon as possible.</p>	<p>Any person who makes a report through the reporting channel as above will receive a written acknowledgement of his/her report through SMS or email.</p> <p>We will endeavour to recover the sum sent in error from the recipient and inform you of the outcome.</p> <p>Complicated cases may require a longer time, but we will update you of the outcome accordingly.</p>

10. If I report an unauthorised transaction, am I still liable for the transaction?

You will not be liable for any loss that arises from any action or omission by us if you have complied with your duties as an account holder. For losses arising from any action or omission by any third party other than you and us, you will also not be liable for the first S\$1,000.

You will, however, be liable if it is ascertained that the primary cause was recklessness on your part., In such instances, your liability will be capped at the transaction limit or daily payment

limit, where applicable. Examples of conduct that constitute recklessness and could lead to losses from unauthorised transactions include:

- a. Storing your access code in a manner that can be easily assessed by any third party;
- b. Knowingly sharing or surrendering access codes to non-operators of your account, resulting in completed transactions;
- c. Ignoring notifications, alerts or warnings from us;
- 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 we have:
 - i. specifically instructed you not to do so; and
 - ii. warned you of the consequences of doing so.

In all cases, we will conduct an assessment to determine the appropriate liabilities and work towards a fair and reasonable resolution. We will also communicate the claim resolution process and assessment to you in a timely and transparent manner.

11. What should I do if I receive erroneously sent funds?

You should report to us as soon as practicable. You may be facilitating criminal activities, such as money laundering and unlicensed moneylending, if you knowingly receive money from strangers, dubious sources or other unverified sources. It is a criminal offence if your bank account is used to receive money linked to criminal activities or keeping erroneously sent funds.

12. What are the duties of ANEXT Bank?

We will ensure that:

- we inform every account holder and account operator of a protected account of their user protection duties
- we inform every account holder and account operator of a protected account of the risks and implications of performing high-risk activities
- we provide a self-service feature for every account holder to promptly block further access to a protected account
- we send outgoing notification alerts to every account holder on a real time basis for each transaction and whenever a high-risk transaction is performed by way of SMS and email

- we provide an onscreen opportunity for you to check the recipient credentials before executing any authorised payment transaction
- we have capabilities in place to detect and block suspected unauthorised transactions at all times
- we provide you with a reporting channel for the purposes of reporting any unauthorised or erroneous transaction(s)
- we strive to assist you promptly, professionally and fairly with these service standards:
 - Your query or feedback will be responded to within three (3) business days.
 - We aim to complete our investigation of any non-complex claim in relation to any unauthorised transaction within 20 business days.
 - Sole proprietors may reach out to the [Financial Industry Disputes and Resolution Centre Ltd](#) using the channels listed under Contact Us at <https://www.fidrec.com.sg/contact-us> if disagreements arise from resolutions.