VP Bank Ltd Singapore Branch
128 Beach Road · #13-01 Guoco Midtown · Singapore 189773 · Singapore
T +65 6305 0050 · info.sg@vpbank.com · www.vpbank.com
Business Registration No. T18FC0095B · GST Registration No. M90372316T

User Protection Duties Applicable in relation to Individual Accountholders on E-payments

(Applicable only if the payments function is enabled for e-banking services)

1. General Overview

This document contains information pursuant to the E-Payments User Protection Guidelines (as amended or superseded from time to time, the **"E-Payments Guidelines"**) issued by the Monetary Authority of Singapore (MAS). The E-Payments Guidelines set out guidelines for financial institutions in Singapore in relation to electronic payment transactions (**"e-payments"**) done via accounts where the accountholders are individuals or sole proprietors. If you are an individual accountholder (whether in your sole name or jointly) with VP Bank Ltd Singapore Branch (the "**Bank**") or an individual holding an account with the Bank for your sole proprietorship business, then the information set out in this document will apply to you.

This document is not a contract. However, the information in this document mirrors the additional terms and conditions contained in the section labelled "*Additional Terms and Conditions Applicable in relation to Individual Accountholders on E-payments*" (the "**ATCs**") appended to the Bank's e-banking application form titled "*Application for use of e-banking services form*" (the "**e-banking form**").

The ATCs must be read in the overall context of the other terms and conditions governing banking facilities and services as provided by the Bank. Further, capitalised terms used in the ATCs (and which are also therefore used here in this document) have the same meaning as defined in the Bank's Account Agreement. Therefore, please refer to the e-banking form as well as the relevant contractual documents mentioned in the e-banking form, for the definitions of all the capitalised terms.

2. Transaction Notification Alerts

In this document, the term **"Users"** shall refer collectively to the Client and the Participant (and if applicable, the Additional User(s), such capitalized terms as defined in the Bank's Terms and Conditions for e-banking^{plus}).

Post-transaction push notifications to confirm transactions that were done using the e-banking portal, including e-payments, are enabled by default. The User may, via the e-banking portal, set up and make adjustments to post-transaction push notifications (including deleting or temporarily disabling).

It is the Client's responsibility to enable and monitor, or ensure that the Users enable and monitor, transaction notification alerts. The Bank may, where the system permits, comply with the User's preferences on the transaction notification alerts.

Further information on the e-banking portal and updates with respect to (amongst other things) system capabilities allowing such adjustments of the Client's preferences, is available at https://www.vpbank.com/en-sg/private-clients/e-services/e-banking.

3. Users to Protect Access and to Report Unauthorised and Erroneous Transactions

Users to Protect Security Codes

3.1 Users should not:
- a) voluntarily disclose Security Codes to any third party, including the staff of the Bank;
- b) disclose Security Codes in a recognizable way on any account, Security Device or any container for the Account(s) (where relevant); or
- c) keep a record of Security Codes in a way that allows any third party to easily misuse them.

3.2 Users should make reasonable efforts to secure any record of Security Codes, including keeping the record in a secure electronic or physical location accessible or known only to the User, and where the record is unlikely to be found by a third party.

Users to Protect Access

3.3 Users should also:
- a) download the Bank's mobile application from official sources;
- b) update browsers on any device used to access the Accounts, to the latest version available;
- c) patch the device's operating system with regular security updates provided by the operating system provider;
- d) install and maintain the latest anti-virus software on the device, where applicable;
- e) use strong passwords such as a mixture of letters, numbers and symbols or strong authentication methods (such as (where available) fingerprint authentication methods);
- f) not root or jailbreak the device(s) used; and
- g) not download and install applications from third party websites outside official sources, particularly unverified applications which request device permissions unrelated to their intended functionalities.

0019_EXT_GN_SG_EN/241213/ARC_7331

VP Bank Ltd Singapore Branch
128 Beach Road · #13-01 Guoco Midtown · Singapore 189773 · Singapore
T +65 6305 0050 · info.sg@vpbank.com · www.vpbank.com
Business Registration No. T18FC0095B · GST Registration No. M90372316T

3.4 Clients should inform all Users of the security instructions or advice provided by the Bank and all Users should adhere to such instructions or advice.

User to refer to official sources to obtain website addresses and phone numbers

3.5 Users should refer to official sources (such as the MAS Financial Institutions Directory) to obtain the Bank's website addresses and phone numbers. In this regard, the Bank should ensure that its details as listed in the MAS Financial Institutions Directory, are up to date.

Clients to report unauthorised transactions

3.6 E-payments in relation to Accounts initiated without the knowledge (actual or imputed) and consent (express or implied) of the Users, are **"unauthorised transactions"**. For the avoidance of doubt, unauthorized transactions do not include the following: (a) if a User knows of and intended to make the e-payment, the e-payment is not an unauthorised transaction notwithstanding that the transaction could have a arisen as a result of the User falling victim to a scam; and (b) if the Client had shared access and usage of his/her device with another person or stored that person's biometrics identities on his/her devices, and that other person had then performed the e-payment, the Client is deemed to have consented to such use of the Account by that other person and the payment was therefore not an unauthorized transaction. However, unauthorized transactions include transactions that are seemingly authorized transactions. Seemingly authorized transactions refer to any e-payments perpetrated through the impersonation of a legitimate business or government entity (the "impersonated entity"), done by a scammer who obtains the User's account credentials via digital messaging platforms by pretending to be the impersonated entity, the User enters his/her account credentials on a fabricated digital platform such as a website or application and these fraudulently obtained credentials are then used to perform transactions that the User does not intend to perform.

3.7 Clients should report any unauthorised transactions through the Bank's reporting channel at **customercare.sg@vpbank.com** as soon as practicable and no later than 30 days after receipt of the relevant notification alert of the unauthorized activity, and should further provide the Bank with reasons if the report is delayed. The reporting channel is free of charge and you will receive an acknowledgement upon making a report. Clients should also make a police report if so requested by the Bank to facilitate the claims investigation process.

3.8 The E-Payments Guidelines require Clients to cooperate by providing, where requested, the following information to the Bank within a reasonable time in relation to an unauthorised transaction: (a) the affected Account, and any accounts with other banks or financial institutions that have been affected; (b) the Client's identification information; (c) the Security Devices and Security Codes used; (d) the Users' names and identities; (e) where applicable, date and time of loss, theft or misuse of the Account, Security Devices and Security Codes and dates and times of reports to the Bank and the police; (f) how Security Codes were recorded and whether these were disclosed; (g) any other relevant information, such as (where relevant) a description of the scam incident, details of remote software downloaded as instructed by scammers, whether any passwords or notifications were sent by the Bank and any confirmations from telco service providers (where feasible to obtain), and any suspected compromised applications on the User's device(s).

Users to Report Erroneous Transactions

3.9 Where e-payments initiated by the Client or Users result in moneys being placed with or transferred to the wrong recipient (**"erroneous transactions"**), Clients should inform the Bank upon becoming aware of the same and shall render full cooperation to the Bank towards the recovery of sums sent in error. These include providing the Bank, upon request, with the information in section 3.8 above (where applicable), the recipient's unique identifier (including account number, identification number, name or other credentials entered by User) and the date, time, amount and purpose of the erroneous transaction.

Clients to provide the Bank with contact information for notifications and other matters

3.10 Clients should provide the Bank with contact information as may be required so that the Bank may set up notification alerts.

0019_EXT_GN_SG_EN/241213/ARC_7331

VP Bank Ltd Singapore Branch
128 Beach Road · #13-01 Guoco Midtown · Singapore 189773 · Singapore
T +65 6305 0050 · info.sg@vpbank.com · www.vpbank.com
Business Registration No. T18FC0095B · GST Registration No. M90372316T

4. The Bank to Facilitate User Protection

4.1 The Bank has provided Users with an onscreen opportunity for Users to confirm e-payments before the e-payment is actually executed, where the following would be provided (a) information allowing the user to identify the account to be debited (b) the intended e-payment amount, and (c) details of the intended recipient (such as account number or registered payee name). Users should take note of the obligations in clause 3.1 above, and ensure that any Security Code should not be revealed to third parties, even if this is not specifically highlighted in any pre-transaction confirmation arrangements.

4.2 The Bank shall ensure continued delivery of key services and alternatives during any scheduled system downtimes, and that any such downtimes are not performed where a high volume of transactions are expected.

5. Client Liability for Certain Losses

5.1 For the avoidance of doubt, section 5 herein does not in any way supersede or render ineffective any of the provisions in Part IV (including without limitation the provisions in connection with the Bank's exclusions of warranty and liability and the Client's obligations to indemnify the Bank), save that where the Client's liability with respect to e-payments under the provisions of Part IV is higher than as provided in this section 5, the lower liability as provided in this section 5 shall prevail.

5.2 Where an e-payment was an authorized transaction (including where the User had acted fraudulently to defraud a Client or the Bank), the Client shall be liable for the same. If there was any transaction limit set or agreed with the Bank, the Client shall be liable up to any such transaction limit.

5.3 Where an unauthorised transaction is involved and the primary cause of any actual loss was recklessness on the part of the Users, the Client shall be liable for the actual loss which may (if any transaction limit was set or agreed with the Bank) be an amount up to such agreed transaction limit or the entire amount of loss (if such transaction limit was not applicable). Recklessness shall include failure to adequately protect access to Security Codes, ignoring notifications, alerts or warnings from the Bank, selecting easily recognizable Security Codes where specifically warned not to do so, and retaining sideloaded apps which are unverified or request device permissions unrelated to their intended functionalities. In this regard, Users should provide the Bank with information the Bank reasonably requires to determine whether any User was reckless.

5.4 Where a loss arises in an unauthorized transaction and such loss arises from an action or omission by the Bank as described in (a) and (b) below and not from a failure by a User to comply with his duties as mentioned herein, the Client shall not be liable for the loss. The term any "action or omission by the Bank" shall mean the following:

a) fraud or negligence by the Bank, its employees, agents or any outsourcing service providers contracted to provide the Bank's services through the Account;
b) non-compliance by the Bank or its employees with any requirement imposed by the MAS in relation to the Bank's provision of a financial service; and
c) non-compliance by the Bank with the duties set out in section 4 of the E-Payments Guidelines.

5.5 If a loss from an unauthorised transaction arises due to any action or omission by a third party who/which is not the Bank's agent or outsourcing service provider (please see section 5.4(a) above), and such loss does not arise from a failure by a User to comply with his duties as mentioned herein, the Client shall not be liable for the first S$1,000 of loss arising from an unauthorised transaction.

6. Unauthorised Transactions – Client Claims Assessment

6.1 Client claims in relation to any unauthorised transaction (a **"relevant claim"**) will be assessed by the Bank to see if section 5 above will apply. Even if section 5 is assessed as not applying to a relevant claim, the Bank shall endeavour to resolve the relevant claim in a fair and reasonable manner and shall communicate the claims resolution process and assessment to the Client in a timely and transparent manner.

6.2 The Bank may require the Client to furnish a police report in respect of the relevant claim, prior to initiating the claims resolution process. In this regard, the Bank may, upon the Client's request, provide information on the procedure to file the police report. The Client should also make a police report if the Client suspects that he/she is a victim of scam or fraud. If the Client so requests, the Bank may provide the Client with information on the procedure to file the police report, as well as relevant information that the Bank has on the unauthorised transactions (including transaction dates, timestamps and parties to the transaction). In this regard, the Client should cooperate with the police and provide evidence where practicable. The Client should also furnish the police report to the Bank within 3 calendar days upon request, in order to facilitate the Bank's claims investigation process.

0019_EXT_GN_SG_EN/241213/ARC_7331

VP Bank Ltd Singapore Branch
128 Beach Road · #13-01 Guoco Midtown · Singapore 189773 · Singapore
T +65 6305 0050 · info.sg@vpbank.com · www.vpbank.com
Business Registration No. T18FC0095B · GST Registration No. M90372316T

6.3 Where, pursuant to the Bank's investigations, the Bank has assessed that the Client is not liable for a loss arising from the unauthorised transaction, the Bank shall credit the Account with the relevant amount.

6.4 The Bank shall endeavor to complete an investigation of a relevant claim within 21 business days (for straightforward cases) or 45 business days (for complex cases). The Bank will inform the Client of the applicable investigation timeline as well as the arrangements in section 6.2, upon receipt of the Client's report of an unauthorised transaction. Within the applicable investigation period, the Bank shall provide the Client with a written or oral report of the investigation outcome and the Bank's assessment of the Client's liability, which shall be acknowledged by the Client.

6.5 It is the aim of the Bank to resolve Client claims as fairly, efficiently and amicably as possible. However, in the event the Client disagrees with the Bank's assessment, the Client may raise an objection via **customercare.sg@vpbank.com** or pursue other modes of dispute resolution (including mediation at Financial Industry Disputes Resolution Centre ("FIDReC").

0019_EXT_GN_SG_EN/241213/ARC_7331