One-time Password Terms and Conditions

Article 1. Definitions

“Token” means a smartphone application or device provided by PayPay Bank Corporation (“Bank”) to a holder of a PayPay Bank ordinary deposit account (such holder is called “Customer”, and such account is called “Bank Account”), which generates passwords for transactions with the Bank. “One-time Password” means a temporary random password that is generated and indicated by a Token.

Article 2. Ownership of Tokens; No Assignment or Other Transfer of Tokens

The ownership of the Tokens shall belong to the Bank. The Bank shall provide the Customer with a Token. The Customer is not allowed to assign, provide as security or otherwise grant any other right in a Token to any third party, lend a Token to any third party or allow any third party to possess or use a Token.

Article 3. Provision of Token

1. As a rule, the Bank shall assign and provide the Customer with one Token. When the Customer who meets the requirements specified by the Bank requests to use two or more Tokens by the method specified by the Bank, or the Bank deems it necessary, the Bank shall assign and provide the Customer with an additional Token. The maximum number of additional Tokens allowed per Customer shall be as separately specified by the Bank.
2. When a Token provided by the Bank pursuant to Article 3.1 has been lost or damaged and the Customer wishes to receive a replacement Token, the Customer must request the replacement Token by the method specified by the Bank. The Bank shall accept such request when the Bank considers that the Customer needs a replacement Token.
3. Notwithstanding Articles 3.1 and 3.2, the Bank shall not provide the Customer with a Token when:
   (1) any mail sent to the address the Customer provides to the Bank (“Customer’s Address”) is undeliverable as addressed, or otherwise the Bank considers that the Customer’s whereabouts are unknown;
   (2) the Customer does not use the Customer’s Bank Account for the period specified by the Bank; or
   (3) otherwise the Bank considers that it is not appropriate to provide the Customer

with a Token.

4. The Customer agrees to pay the Token fee as separately specified by the Bank, if any, when the Customer receives a Token from the Bank. Notwithstanding the PayPay Bank Account Terms and Conditions, the Bank reserves the right to automatically withdraw the Token fee from the Customer's Bank Account on the day specified by the Bank without obtaining the Customer's consent or approval online, by phone or in writing.

Article 4. Enabling One-time Password Authentication

1. To use the One-time Password for authentication of the Customer by the Bank, the Customer must use a Token provided by the Bank to enable the One-time Password authentication by the method specified by the Bank.
2. When the Bank confirms that the Customer's information sent to the Bank is consistent with the Customer's information retained by the Bank by the method specified by the Bank at the time when the Customer enables the One-time Password authentication, the Bank shall deem that the Customer has enabled the One-time Password authentication and use the One-time Password to authenticate the Customer for the transactions specified by the Bank which the Customer makes at or after the time specified by the Bank.

Article 5. Using One-time Password

1. When the Bank confirms that the Customer's information electronically sent to the Bank is consistent with the Customer's information retained by the Bank by the method specified by the Bank to authenticate the Customer after the Customer enables the One-time Password authentication, the Bank shall deem that the Customer requests to make a transaction related to the authentication. Even if such transaction request is not made by the Customer, the Bank shall not be responsible or liable for any damage caused by the transaction in question.
2. The Bank reserves the right to require the One-time Password authentication for the transactions specified by the Bank whenever the Bank deems it appropriate. When the Bank requires the One-time Password authentication, the Customer will not be able to make such transactions if the Customer fails to receive a Token from the Bank or fails to enable the One-time Password authentication even after receiving a Token from the Bank.
3. When the Bank authenticates the Customer, if the Customer's information electronically sent to the Bank is not consistent with the Customer's information

retained by the Bank, the Bank shall temporarily disable the One-time Password authentication for the Customer after the number of consecutive unsuccessful attempts specified by the Bank.

4. The Customer shall be entitled to request the Bank to enable the One-time Password authentication even if it is disabled pursuant to Article 5.3 by following the procedures specified by the Bank. When the Bank considers that it is appropriate to enable the One-time Password authentication for the Customer, the Bank shall accept the Customer's request and enable the One-time Password authentication.
5. The Bank reserves the right to immediately suspend or restrict the use of the One-time Password functions for authentication of the Customer without notifying the Customer in advance when the Bank has any doubt regarding the security of the One-time Password due to malfunction of the Tokens or other reasons. Upon suspension or restriction of the use of the One-time Password functions, the Bank reserves the right to specify other authentication procedures (such as use of Login IDs or execution of a fixed-term BA-PLUS agreement) for any and all transactions which require authentication, and the Customer agrees to follow such procedures. The Bank also reserves the right to change the Customer's daily funds transfer limit without obtaining the Customer's approval.

Article 6. Notification of Loss or Theft of Token or One-time Password

1. The Customer shall be responsible for keeping the Tokens and the One-time Password strictly confidential.
2. When the Customer loses a Token; a Token or the One-time Password is likely to be used by others as a result of counterfeit, forgery, theft or loss of the Token or the One-time Password; or it is discovered that a Token or the One-time Password is used by others, the Customer must immediately notify the Bank by the method specified by the Bank.
3. When the Bank receives the notification specified in Article 6.2, the Bank shall promptly suspend the use of the One-time Password generated by the Token notified as lost, counterfeited, forged or stolen for authentication of the Customer. The Bank shall not be responsible or liable for any damage incurred prior to the receipt of notification under Article 6.2 by the Bank.

Article 7. Expiration Date of Token

As a rule, a Token shall expire on the date specified by the Bank.

Article 8. Other Applicable Terms and Conditions

Any matter not specified in these Terms and Conditions shall be subject to the PayPay Bank Account Terms and Conditions.

Article 9. Amendment of Terms and Conditions

1. The Bank shall amend any provision of these Terms and Conditions or other terms and conditions in accordance with Article 548-4 of the Civil Code of Japan when the Bank deems it reasonably necessary to respond to any change in economic or other circumstances, or for other reasons.
2. When the Bank amends any provision of these Terms and Conditions or other terms and conditions pursuant to Article 9.1, the Bank shall announce the amendment as well as the details and effective date of the amened provision by publication on the internet or by other reasonable means.
3. The amendment under Articles 9.1 and 9.2 shall take effect on the effective date specified at the time of publication. The Bank shall provide a reasonable period between the date of publication and the effective date depending on the details of the amendment.

[January 18, 2024]

*In the event of any discrepancy or inconsistency between the English and Japanese versions of these Terms and Conditions, the Japanese version will prevail.