Get to Know 3D Secure & Non 3D Secure **Transactions Protocol** from Permata Debit Plus

To avoid criminal activities while doing online shopping transactions (e-commerce), PermataBank has been implementing the 3D Secure (3DS) security technology from Visa. 3D refers to the 3 domains, consisting of the card Issuer, merchant, and 3DS transaction processor.

Here are some things to know about 3DS & Non-3DS transaction types.

A. Debit Card Transaction Authorization Types Based on the security protocol, online shopping transactions are divided into 2 types,

namely: 3DS and Non-3DS transactions.

3D Secure Transactions



The online shopping transaction with 3DS will take place WITH an additional transaction authorization code in the form of an SMS OTP (one-time passcode). The 3DS system will automatically send an SMS OTP to the PermataDebit Plus Cardholder for every transaction, and subsequently, the card holder will enter it on the transaction verification page (marked: Verified by Visa) as approval or authorization for the transaction by Permata Debit Plus Cardholder.



The online shopping transaction conducted with the mataDebit Plus card WITHOUT 3DS authentication,

Non-3D Secure Transactions

does not require any additional transaction authentication in the form of an SMS OTP. The transaction is processed by the merchant without relying on the 3DS system. To ensure the safety of the Customer in making online transactions with Permata Debit Plus,

the Bank (with certain considerations) may place restrictions on online transactions without prior notification to the Cardholder. Therefore, the Bank is released from all claims due to restrictions on transactions that occur.

For 3DS transactions, both points must be fulfilled, whereas for Non-3DS transactions,

B. Terms & Conditions for 3DS & Non 3DS Transactions

only the first point is sufficient.



has Verified by Visa status.

merchant.

details:





Oo to the online merchant's official website, make sure the merchant

C. How to Do Online Transactions with PermataBank Debit Card

- 2 Select the product you wish to buy. 3 Proceed to the payment menu and select credit/debit card payment. Then, proceed with the next steps as instructed by the online
- Debit card number - Debit card expiration date

4 For debit card payments, Customers need to enter the following card

- 3-digit CVV code of the debit card (printed on the back of the card)

D. Tips for Avoiding Debit Card Misuse

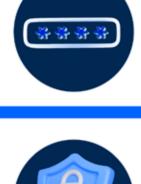
Use a Private Network

unauthorized access to your personal data.

Merchants, Support for 3D Secure. Make sure you only make transactions at verified merchants that provide 3D Secure services.

Shop at Official Websites of Trusted

Avoid using public Wi-Fi networks when making online transactions with the PermataDebit Plus card. Public Wi-Fi networks may provide an opportunity for fraudsters to gain



from those claiming to be Bank employees/officers. This is a common type of fraud used to deceive customers.

Do Not Share OTP-Response Code

Enable Two-Factor Authentication (2FA) on Online Merchant Accounts

The 2 FA feature provides extra security for your account,

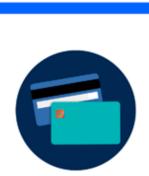
Always keep the OTP-Response Code confidential, including



Subscribe to SMS Navigator Service

reducing the chance of breach attempts.

Customers are advised to subscribe to the Navigator SMS service, which allows Customers to receive notifications for transactions on their account that exceed Rp500.000.



Customers can perform account separation according to their

Separation of Your Banking Accounts

needs, such as: Customers can provide funds according to the needs of

online transactions that will be carried out using a debit card.

- Accounts for savings and other needs (with a PermataDebit Plus card with the GPN logo) that do not yet support online
- By separating banking accounts, the Customer can minimize potential losses due to debit card misuse by fraudsters.

telephone, or email on behalf of **Permata**Bank, you can contact:

debit transaction services.



care@permatabank.co.id @PermataCare

If you get a suspicious chat from Facebook/Instagram/TikTok/WhatsApp/Telegram, SMS,



