FAQs on Double-Swiping

All retail merchants in Singapore are required by The Association of Banks in Singapore (ABS) and the Card Schemes (i.e. American Express, Diners Club, JCB, MasterCard, UnionPay and Visa) to stop capturing and storing sensitive payment card data (or cardholder data) encoded on the magnetic stripes of customersô payment cards (i.e. credit, debit and charge card).

Since early 2012, ABS and its member banks have reached out to the retail merchants in Singapore to advise them not to capture or store cardholder data. Retail merchants have since stopped doing so. ABS and its member banks will continue to monitor and educate the retail merchants.

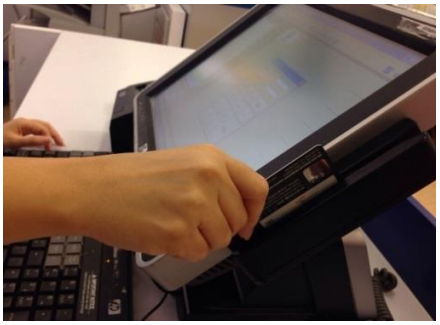
1. What is double-swiping?

Double-swiping is the capturing of payment card data encoded on the magnetic stripes of customersô payment cards at the Point-of-Sale (POS) reader / Electronic Cash Register (ECR). The data is captured when a payment card is swiped on a retail merchantôs POS reader / ECR. Double-swiping is **not a required step** in a payment transaction.

Example A - double-swiping, or reading the magnetic stripe of the card at POS reader/ ECR.

Example B - inserting or dipping a chip-enabled payment card in a payment card terminal for payment is **not** considered as double-swiping.

A



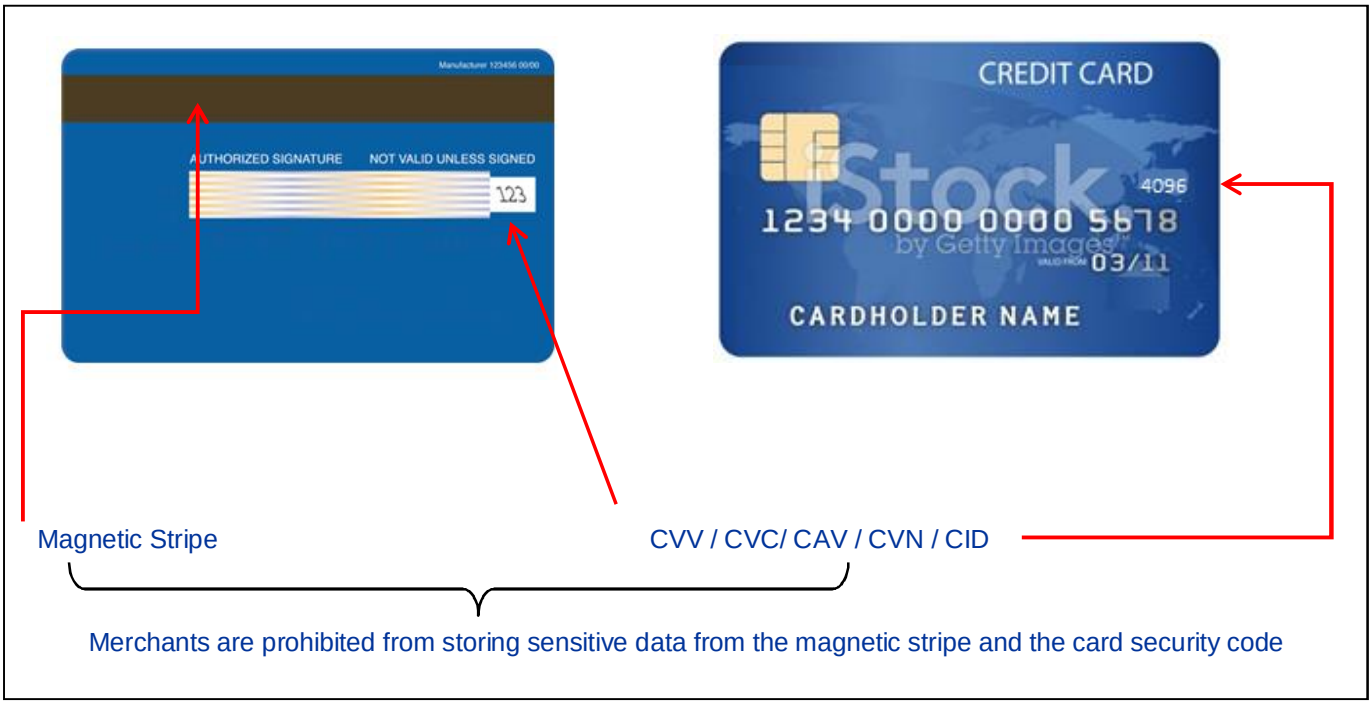
B

2. What are the sensitive payment card data that merchants should not store?

Sensitive payment card data such as card security code (CVV/CVC/CAV/CVN) are encoded on the magnetic stripes of payment cards. Retail merchants should not store such data.

The card security code goes by different names under the various Card Schemes as follows :

Card Identification Number (CID) ï American Express;
Card Authentication Value (CAV) ï JCB;
Card Verification Code (CVC) ï MasterCard;
Card Verification Number (CVN) ï UnionPay;
Card Verification Value (CVV) ï Visa/Diners.



3. What are the risks of double-swiping or storing of payment card data by merchants?

Fraudsters can install malicious programmes on merchantsôPOS readers / ECR to steal sensitive payment card data.

The stolen payment card data can then be used to produce counterfeit cards or make fraudulent online purchases. As a result, cardholders may suffer financial losses.

There is also the risk that the data stored by the retail merchant is stolen and misused.

4. Why can't the magnetic stripes be removed from payment cards since all local POS magnetic stripe transactions for Singapore-issued payment cards have ceased?

EMV chip technology is not adopted in some countries. Card transactions at retail merchants in these countries can therefore only be completed by using the information that is encoded on the magnetic stripes of payment cards.

5. What can I do to reduce the chance of my payment card data encoded on the magnetic stripe being fraudulently used at overseas retail merchants?

To minimise unauthorised transactions, you should activate the magnetic stripe on your card only for the period that you are travelling overseas.

6. What should I do if I suspect a Singapore-based retail merchant has double-swiped my payment card?

You should report the incident or any attempt of double-swiping by a merchant to ABS via email: banks@abs.org.sg. ABS will look into the matter, and identify the retail merchant that does not comply with the ñdo not double-swipeòrule set out by ABS and the Card Schemes.

If you suspect that your personal data has been collected by the retail merchant without your consent and for purposes other than the payment transaction, you may report the matter to the Personal Data Protection Commission, or PDPC, via email: info@pdpc.gov.sg.

Please include the following details in your email:

(a) Date and time of your transaction;

(b) Name of the merchant outlet; and

(c) Address of the merchant outlet.