pdpc

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

GUIDE ON THE PRACTICE OF PASSING MAGNETIC STRIPES OF PAYMENT CARDS THROUGH A READER

21 APRIL 2016

GUIDE ON THE PRACTICE OF PASSING MAGNETIC STRIPES OF PAYMENT CARDS THROUGH A READER

1. In Singapore, all credit, debit, charge, or NETS payment cards are microchip enabled for payment using card readers. Hence, it is no longer necessary to pass the magnetic stripes on these cards through card readers to make payment. The act of passing the magnetic stripes on such cards through a card reader is referred to as "swiping" or "double-swiping".

2. The Personal Data Protection Commission ("**PDPC**") had received enquiries from individuals about merchants swiping the magnetic stripes of the payment cards after payment had been processed through the use of the embedded microchips on the cards.

3. The act of accessing personal data stored in a payment card, through any microchip, magnetic stripe reader or any other means, constitutes collection of the personal data under the Personal Data Protection Act 2012 (the "**PDPA**"), even if the personal data is retained only temporarily by the merchant.

4. Merchants will have to ensure that the collection and use of the personal data in a payment card complies with the obligations in the PDPA. For example, merchants may only collect personal data for purposes that a reasonable person would consider appropriate in the circumstances.

5. When an individual provides a payment card to a merchant for the purpose of making payment, the individual would be deemed to have consented to the merchant processing the personal data stored in the card for that purpose. Generally speaking, the PDPC considers that the activities outlined in **Annex A** are part of the purpose of processing payment.

6. Merchants must protect any personal data collected by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks.

7. The Association of Banks in Singapore (ABS) and the Card Schemes (i.e. American Express, Diners Club, JCB, MasterCard, UnionPay and Visa) have required all retail merchants to stop capturing and storing sensitive payment card data (or cardholder data) encoded on the magnetic stripes of customers' payment cards (i.e. credit, debit and charge card). Please see **Annex B** to this Advisory for the FAQ on Double-Swiping issued by ABS in 2015.

8. Merchants are advised to align their card payment practices with the position in the ABS FAQ while ensuring that they continue to comply with the requirements under the PDPA.

Annex A

Merchants have cited these activities as necessary for the purpose of processing payment:

– Activities related to record keeping for merchant’s accounting processes e.g. generation of sales receipt.

– Activities directly related to completion of the payment transaction e.g. accounting reconciliation of sales necessary for settlement of card transactions with issuing banks.

– Activities related to the resolution of billing disputes or discrepancies e.g. record retention for verification in the event of queries, discrepancies or disputes.

Annex B

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 customers' 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 customers' 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 merchant's 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

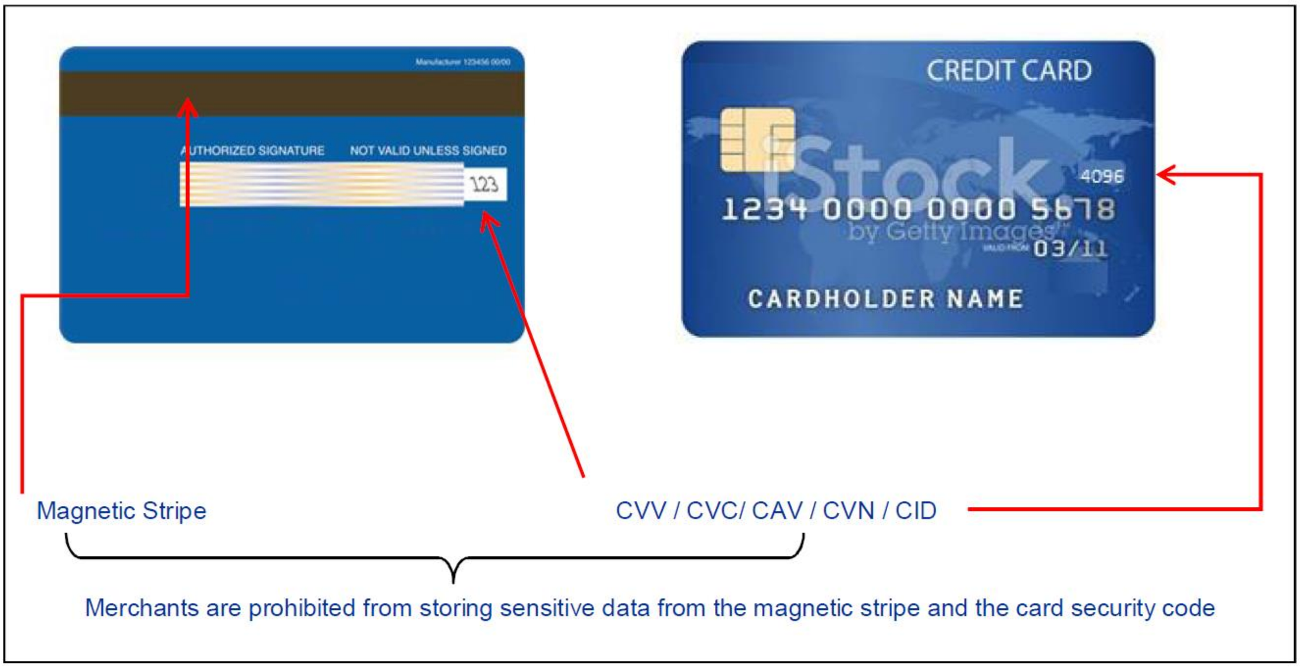
B

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) – American Express;

Card Authentication Value (CAV) – JCB;
Card Verification Code (CVC) – MasterCard;
Card Verification Number (CVN) – UnionPay;
Card Verification Value (CVV) – Visa/Diners.


AUTHORIZED SIGNATURE
NOT VALID UNLESS SIGNED
123
CREDIT CARD
4096
1234 0000 0000 5678
03/11
CARDHOLDER NAME
Magnetic Stripe
CVV / CVC/ CAV / CVN / CID
Merchants are prohibited from storing sensitive data from the magnetic stripe and the card security code

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

Fraudsters can install malicious programmes on merchants' POS 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 “do not double-swipe” rule 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.