Merchant Data Security

01 September 2014

Dear Merchants,

Over 50 per cent of consumer expenditure in Singapore is conducted electronically via card payments*. As more consumers choose to pay electronically, both in-store and online, it is vital that merchants take a more active role to protect both their customers and their business from any potential risks.

It has become apparent that some merchants in Singapore are still capturing cardholder data at the point-of-sale (POS) reader/Electronic Cash Register. Also referred to as “track data”, this information is read and captured when a payment card is swiped on a merchant’s POS reader or Electronic Cash Register to capture card details from the magnetic stripe for loyalty/marketing programs, or internal record keeping purposes. This is known as ‘double swiping’.

Separately, for eCommerce transactions, some merchants store the CVV2/CVC2/ CAV2/CVN2 which is the three-digit number printed on the signature panel on the back of a card, or the CID which is the four-digit number located on the front of the card. (See Figure 1)

The risks

One of the main risks associated with a merchant storing card payment data captured at the point of sale is that this information can be vulnerable to theft. Criminals can then attempt to produce counterfeit cards or use the data to make purchases online.

** Euromonitor Merchant Segment Study for Visa, March 2013*

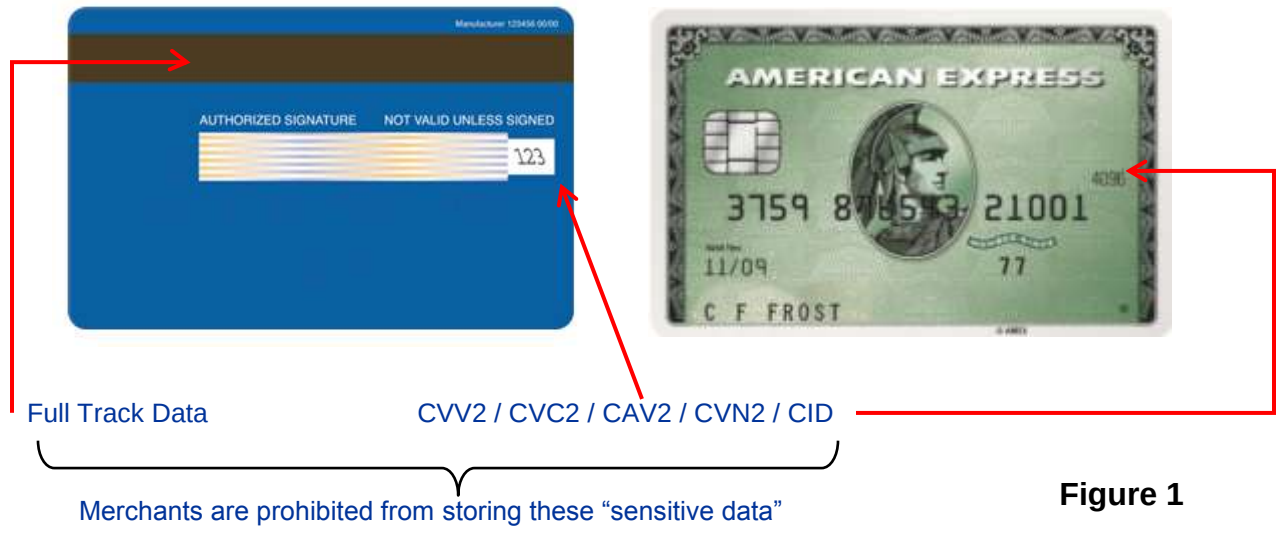

Figure 1

* The three-digit code goes by different names under the various card schemes:
CVV2 – Visa/Diners; CVC2 – MasterCard; CID – American Express; CAV2 – JCB; CVN2 – UnionPay

What are the rules?

The Card Schemes' rules state that merchants are prohibited from:

- At point-of-sale (POS) **–** Storing full track data (magnetic-stripe data) information through swiping the payment card at the POS device (double swiping).

- In the card-not-present environment **–** Storing the Card Security Code (CVV2/CVC2/CAV2/CVN2) number on the signature panel on the back of the card, or the CID number located on the front of the card, post-authorisation. (See Figure 1)

The Association of Banks in Singapore (ABS) together with the payment card industry and the Card Schemes i.e. American Express, Diners Club, JCB, MasterCard, UnionPay and Visa requires merchants to:

(a) take **IMMEDIATE** steps to stop the capturing and storage of prohibited cardholder data that is collected from customers' payment cards; and

(b) speak to your merchant bank representative to discuss alternatives.

Collection of cardholder data for organisation's own use

For the purpose of collecting cardholder data for your organisation's own loyalty/marketing programs, your organisation cannot obtain the information from the magnetic stripe on the payment cards.

Instead, your organisation will need to consider an alternative source of collecting the required information. For that purpose, merchants will need to comply with the Personal Data Protection Act (PDPA), which came into effect on **2 July 2014.**

For more information on the PDPA, please visit the website of the Personal Data Protection Commission at www.pdpc.gov.sg.

Thank you for your co-operation.