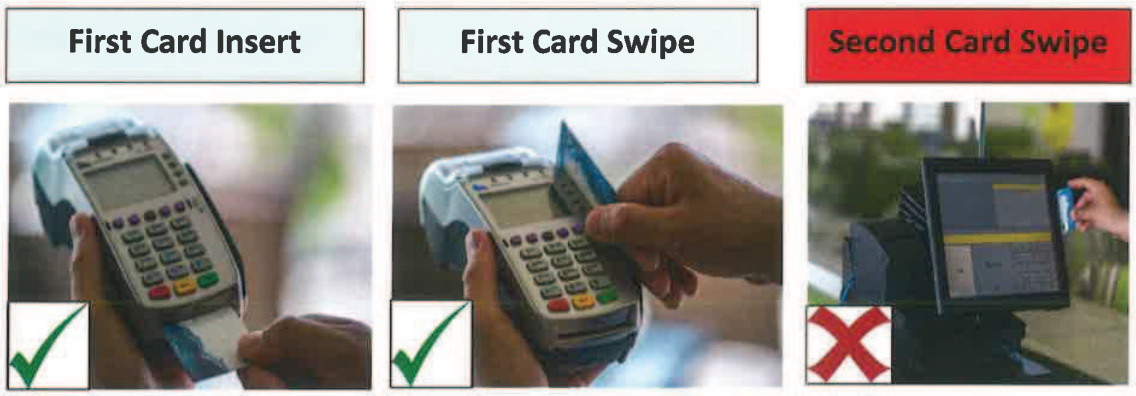
Frequently asked questions (FAQ) on "Double Swiping" of payment cards to be discontinued from 15th June, 2017.

The Central Bank of Bahrain (CBB) has announced that all merchants and shopkeepers in Bahrain are required to stop their present practice of "double swiping" of payment cards such as credit, debit, charge or prepaid cards, at their own point of sale (POS) and cash registers, from 15th June, 2017.

1. **What is "Double Swiping"?**

When a card is first inserted into the point-of-sale (POS) at a sales counter, the card transaction is completed after the necessary approval or denial. The customer immediately receives a transaction advice via SMS.

"Double swiping" means a merchant or shopkeeper swiping a card for the second time at his or her own point of sale (POS) or cash register, immediately after the card transaction is approved in response to the first insert or swipe at a POS belonging to the card acquirer. "Double swiping" is not a part of a card transaction.



2. **Why are payment cards double-swiped?**

Merchants or shopkeepers "double swipe" to collect vital card payment details and cardholders' personal data on magnetic stripes of customers' credit, debit, charge or prepaid cards, for their internal accounting purposes and or marketing purposes.

3. **What vital information can be accessed by double swiping?**

By swiping the card at shopkeeper's own POS or a cash register, it is possible to get access and store all payment cardholder and sensitive authentication data encoded on the magnetic stripe of a customer's payment card. Cardholder data means any personally identifiable data of a cardholder or the customer. This includes the primary account number (PAN), cardholder name, expiration date and service code. Sensitive authentication data means full

track data of the magnetic stripe or equivalent data on a chip, card verification codes and values (CAV2/CVC2/CVV2/CID) PINs, PIN blocks. Storing of sensitive authentication data by merchants or shopkeepers after the authorisation of a card transaction, is prohibited.

4. **Why it is risky to double swipe?**

   By double swiping, a shopkeeper can access and store in his or her computer system, customer's all payment card data, including sensitive information encoded on the magnetic stripe. If the shopkeeper's POS, cash register or computer system can be accessed by criminals or fraudsters, card information can be stolen and counterfeit payment cards can be created and/or fraudulent transactions can be carried out.

5. **Why do EMV chip embedded payment cards issued in Bahrain have magnetic stripes?**

   Card transactions in Bahrain are processed using information in chips and PIN numbers. All payment cards issued in Bahrain under the international brands can be used abroad. Therefore, all cards have magnetic stripes, for the cardholders to use them when they travel to countries where the chip technology has not yet been adopted.

6. **What are the alternative means available for merchants or shopkeepers, who have a valid business need to get the required cardholder data or non-sensitive information?**

   Merchants or shopkeepers, who have a valid business requirement to get the cardholder data or non-sensitive information can consult their acquirers and the vendors of POS machines/ cash registers, to get an integration option, complying with the Payment Card Industry Data Security Standard (PCI DSS).

الأسئلة المتكررة حول وقف ممارسة "التمرير المزدوج" لبطاقات الدفع اعتباراً من 15 يونيو 2017.

أعلن مصرف البحرين المركزي بأنه سيكون على جميع التجار وأصحاب المحال التجارية في مملكة البحرين التوقف عن ممارسة عملية التمرير المزدوج "Double Swiping" لبطاقات الدفع مثل بطاقات الائتمان، أو بطاقات الصراف الآلي، أو بطاقات الدفع المسبق أو ما شابهها في نقاط البيع و صناديق الدفع لديهم، وذلك اعتباراً من 15 يونيو 2017.

1. ما هو التمرير المزدوج "Double Swiping" لبطاقات الدفع؟

عندما يتم إدخال البطاقة في المرة الأولى على جهاز نقطة البيع لدى المحل التجاري تكون العملية قد تمت بشكل كامل بعد الحصول على إشعار قبول أو رفض العملية، ومن ثم يتلقى العميل رسالة نصية على هاتفه الخاص إشعاراً بذلك.

ويقصد بعملية التمرير المزدوج لبطاقات الدفع هو قيام التاجر أو صاحب المحل التجاري بتمرير البطاقة مرة ثانية على جهاز الدفع الخاص به بعد تأكيد عملية السحب على البطاقة استجابة لعملية التمرير الأولى لدى نقطة البيع التي تعود لمزودي أنظمة نقاط الدفع. حيث أن هذا الإجراء ليس جزءاً من عملية الدفع بالبطاقة إطلاقاً.

2. لماذا يتم تمرير بطاقة الدفع مرة أخرى؟

لقد اعتاد التجار وأصحاب المحال التجارية القيام بعملية التمرير المزدوج بهدف جمع تفاصيل بطاقة الدفع والبيانات الشخصية لحامل البطاقة لأغراض محاسبية داخلية و/أو لأهداف تسويقية.

3. ما هي المعلومات الهامة التي يمكن الحصول عليها من خلال عملية التمرير المزدوج لبطاقة الدفع؟

إن التمرير المزدوج لبطاقة الدفع من قبل التاجر أو صاحب المحل التجاري في نقطة البيع الخاص به أو في صندوق الدفع يمكنه من الوصول إلى جميع بيانات بطاقة الدفع، بما في ذلك المعلومات السرية مثل بيانات التحقق ورمز الحماية والبيانات الشخصية المشفرة على الشريط الممغنط، مثل رقم الحساب الأساسي PAN، واسم صاحب البطاقة، وتاريخ الانتهاء، ورمز الخدمة. ويُقصد ببيانات التحقق السرية السجل الكامل المخزن على الشريط الممغنط أو البيانات المشابهة المخزنة على الشريحة الإلكترونية، ورموز التحقق الخاصة بالبطاقة وقيم الـ (CAV2/CVC2/CVV2/CID) PINs, PIN blocks. إن حفظ وتخزين البيانات السرية من قبل التاجر بعد التحقق من عملية الدفع بالبطاقة أمرٌ محظور.

4. ما هي خطورة التمرير المزدوج لبطاقة الدفع؟

إن عملية التمرير المزدوج ستمكن التاجر من تخزين بيانات بطاقة الدفع الخاصة بالعميل، بما في ذلك المعلومات السرية المشفرة على الشريط الممغنط. وبالتالي إمكانية الوصول لهذه البيانات في حال تم الدخول إلى نقطة البيع أو نظام الحاسوب الخاص بصندوق الدفع لدى المحل التجاري من قبل أي شخص مع امكانية تعرض بطاقة العميل للتزوير أو استخدامها لإجراء عمليات دفع مزورة. وبالتالي، فقد برزت الحاجة الماسة لوقف ممارسة التمرير المزدوج لبطاقات الدفع لحماية بيانات حامل البطاقة من السرقة وضمان ثقة الجمهور بمعاملات البطاقات

5. ما السبب في أن بطاقات الدفع من نوع EMV التي تحتوي على شريحة الكرتونية تتضمن شريطاً ممغنطاً؟

يتم معالجة عمليات بطاقات الدفع في مملكة البحرين باستخدام معلومات وأرقام حماية مخزنة على الشريحة الإلكترونية. حيث تمكن صاحبها من استخدامها داخل وخارج مملكة البحرين بشكل آمن. ومع ذلك فإن جميع البطاقات تحمل شريطاً ممغنطاً ليتمكن أصحابها من استخدامها في سفرهم إلى دول لم يتم فيها استبدال الشريط الممغنط بشريحة إلكترونية بعد.

6. ما هي الوسائل البديلة المتاحة للتجار وأصحاب المحال التجارية ممن تتطلب أعمالهم التجارية الحصول على بيانات صاحب البطاقة أو على المعلومات غير السرية؟

يمكن للتجار أو أصحاب المحال التجارية في حال كانت أعمالهم التجارية تتطلب الحصول على معلومات غير سرية عن صاحب البطاقة استشارة مزودي أنظمة وأجهزة نقاط البيع لدمج أنظمتهم وذلك بما يتماشى مع معيار أمن بطاقات الدفع (PCI DSS).