Fubon Bank
富邦銀行

收集及處理於銷售點出示及進行信用卡交易時提供的資料 — 商戶實用錦囊(「實用錦囊」)

I. 導言

一般信用卡正面及背面都印有多項資料，包括持卡人姓名、信用卡號碼、信用卡發出及到期日、驗證碼及持卡人簽署，故此，接受信用卡支付的商戶應確保符合《個人資料(私隱)條例》(「條例」)的一般性規定、及條例附表1之六項保障資料原則的規定，並應制定書面個人資料保障指引、程序及守則。

保障資料原則第1原則要求機構只收集足夠而不超出直接與職能或活動有關目的的個人資料。保障資料原則第4原則要求機構採取所有切實可行的步驟，防止他人未獲准許地或意外地查閱、處理、刪除、丟失或使用機構持有的個人資料。商戶於銷售點處理及進行信用卡交易付款須特別留意與之有關的第1原則和第4原則的要求及以下有關的實用錦囊。

II. 透過終端機進行的信用卡交易及信用卡分期付款安排

A. 符合第1原則要求的實用錦囊

1. 只透過收單金融機構提供的終端機進行信用卡交易，並在處理付款交易時(i)將帶有晶片的信用卡「插入」終端機或在終端機「刷」磁帶卡上的磁帶，以讀取儲存於晶片或磁帶上的信用卡號碼和有效日期資料，然後(ii)輸入交易金額，讓資料直接傳到收單金融機構的系統。商戶並不需要亦不應收集持卡人其他資料用以處理及進行信用卡交易。

2. 切忌以任何形式或透過任何方法(例如透過「刷」帶有晶片的信用卡或在持卡人簽單上為信用卡留底)，在未經持卡人同意下收集信用卡資料進行銷售分析、貨存管理或任何與信用卡交易無關的用途。

B. 符合第4原則要求的實用錦囊

1. 可行情況下盡早更新終端機以提升交易的安全性。

2. 將帶有晶片的信用卡「插入」終端機進行付款交易，而非「刷卡」，以此避免延誤(由於將帶有晶片的信用卡「刷卡」時會引發系統自動提示「插卡」訊息)及喪失「撤單」的權利。

3. 切忌在處理付款交易時「刷」信用卡，除非該卡是磁帶信用卡，或者雖是帶有晶片的信用卡，但因損壞或其他原因而失效。

4. 在實際可行情況下，或應持卡人要求，商戶應在持卡人視線範圍內處理信用卡付款交易。為此，商戶亦可考慮向收單金融機構要求安裝流動終端機，以便在持卡人視線範圍內「插卡」或「刷卡」以進行信用卡支付交易。

5. 妥善存放持卡人簽單的商戶存根於安全地方，確保只有獲授權人士方可取閱，並小心棄置商戶存根，例如在棄置前確保信用卡資料已無法辨識。

6. 如要處理「撤單」要求，可使用商戶存根上的有關編碼。

7. 定期檢討及適時加強保障持卡人資料的系統，並進行常規的保安檢查，以提防不法份子干擾終端機，並有助及早發現不正常情況，如額外佈線。

8. 商戶如發現客戶信用卡資料外洩，應立即通知收單金融機構、並以可行方法聯絡受影響人士，以及個人資料私隱專員公署；若外洩事件涉及刑事成份，應立即通知警方。

9. 為員工提供定期培訓，以加強他們的個人資料保障意識及處理信用卡支付交易的適當程序。

III. 罪行

違反保障資料原則並不直接構成刑事罪行，惟私隱專員可發出執行通知，指令違反的機構採取補救措施。不遵守執行通知屬於刑事罪行，一經定罪，可被判處最高罰款港幣五萬元及監禁兩年。如罪行在定罪後持續，可處每日罰款港幣一千元。

MAB-PT 12/2016

Fubon Bank
富邦銀行

Practical Tips on Collection and Handling of Credit Card Data by Merchants for Card-present Transactions at the Point-of-sale (Practical Tips)

I. INTRODUCTION

Since the front and back of a credit card are printed with various information, including the cardholders' names, credit card numbers, credit card issue and expiry dates, CVV numbers and cardholders' signatures, any merchant accepting payment by credit card should ensure compliance with the requirements of the Personal Data (Privacy) Ordinance ("Ordinance") in general and the six Data Protection Principles in Schedule 1 to the Ordinance. Merchants should have written data privacy policies, procedures and practices in this regard.

Data Protection Principle 1 (DPP1) requires an organisation to collect personal data which is adequate but not excessive for a purpose directly related to its function or activity. Data Protection Principle 4 (DPP4) requires an organisation to take practicable steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or use. Both Principles 1 and 4 are of particular relevance to merchants in handling card-present payments at the point of sale. The following are the tips in this regard.

II. CARD-PRESENT TRANSACTIONS AND CREDIT CARD INSTALMENT PLANS USING CARD ACCEPTANCE TERMINALS

A. TIPS FOR COMPLYING WITH DPP1

1. Use only the card acceptance terminal provided by the relevant acquiring institution for processing the payment transaction (i) by either "dipping" the chip-based card or "swiping" the magnetic stripe card, as the case may be, in order to capture the credit card number and expiry date embedded in the card and (ii) by inputting the transaction amount for direct transmission to the acquiring institution's system. No other data is needed nor should be collected from the cardholder for processing the card-present transaction.

2. Do not collect credit card data for the purposes of sales analysis, inventory management or any other purposes not related to the card-present transaction by any means or in any form (such as swiping a chip-based credit card or creating an imprint of the credit card on the transaction slip) without obtaining prior consent from the cardholder.

B. TIPS FOR COMPLYING WITH DPP4

1. Upgrade card acceptance terminals to accept chip cards as soon as practicable to enhance the security of payment transactions.

2. Always dip, rather than swipe, the chip-based credit card in the card acceptance terminal in processing a payment transaction, to avoid delay (since swiping a chip-based credit card in the terminal would trigger an automatic alert to dip the card instead) and losing the "Charge Back" right.

3. Do not swipe the credit card for processing a payment transaction unless it is a magnetic strip credit card or when the chip on the chip-based credit card is not functioning due to damage or other reasons.

4. Process the credit card payment within the cardholder's sight when operationally and practically feasible, or upon cardholder's request. To this end, merchants may consider approaching their acquiring institutions to install mobile card acceptance terminals so that dipping or swiping of credit cards will not be out of cardholders' sight.

5. Store properly the merchant copy of the sales slip ("Merchant Copy") in a secure area accessible to only selected personnel and discard the Merchant Copies with caution, such as render credit card data unreadable prior to discarding.

6. Use the relevant codes on the Merchant Copies in handling any "Charge Back" requests.

7. Review regularly and, as appropriate, enhance the relevant systems in safeguarding cardholders' data and apply routine security check to prevent thieves from tempering card acceptance terminals and to identify abnormalities, such as extra wiring.

8. Promptly notify your acquiring institution(s), the affected individual(s) by appropriate means and the Office of the Privacy Commissioner for Personal Data, Hong Kong in the event of data leakage and report the case to the Hong Kong Police Force if it involves a criminal element.

9. Provide regular training to staff to strengthen their awareness of privacy protection and proper card acceptance procedures.

III. OFFENCE

Non-compliance with Data Protection Principles does not constitute a criminal offence directly. The Privacy Commissioner for Personal Data, Hong Kong may serve an Enforcement Notice to direct the organisation to remedy the contravention. Contravention of an enforcement notice is an offence which could result in a fine of HKD50,000 and imprisonment for 2 years. If the offence continues after the conviction, the organisation is liable to a daily penalty of HKD1,000.

MAB-PT 12/2016