CMSGu2012-04

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Debit or Credit Cards Usage

CERT-MU

National Computer Board
Mauritius

April 2012

Issue No. 4

Version 1.1

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this document is to provide an overview of the bank cards available for use today and their security aspects in terms of access.

1.2 Audience

The target audience include all users of bank cards, including debit and credit cards.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 provides a background bank cards.

Section 3 comprises the security issues around bank cards and the solutions.

Section 4 concludes the document.

Sect*ion 5* comprises a list of references that have been used in this document.

Appendix A defines a set of acronyms used in this document.

2.0 Background

A bank card is primarily a card issued by a bank and linked with an individual’s bank account. Bank cards are made of plastic with magnetized strips and are linked to actual funds on deposit. There are different types of bank card in use, ranging from cards which can only be used to access someone’s account through an Automatic Teller Machine (ATM), for example debit cards, to cards which are used just like credit cards for purchases. Depending on the bank that someone banks with, he or she may be offered several choices of bank card when opening an account.

2.1 Debit Cards

Debit cards allow people to pay for purchases quickly, without writing checks or having to make sure they are carrying enough cash. As long as you do not overdraw your account, debit cards are a good way to pay for purchases without borrowing money and paying interest. You can use a debit card when you make a purchase at shops or to withdraw cash from your bank’s ATM, which generally involves no charge. A debit card is safe in that you do not need to carry large amounts of cash that may be exposed to loss or theft.

2.2 Types of debit card systems

There are currently three ways that debit card transactions are processed: EFTPOS, (also known as online debit or PIN debit), offline debit (also known as signature debit) and the Electronic Purse Card System. A single physical card can include the functions of all three types, so that it can be used in distinct ways.

Although many debit cards are of the Visa or MasterCard brand, there are many other types of debit card, each accepted only within a particular country or region, for example “Switch” (now “Maestro”) and “Solo” in the United Kingdom or “Carte Bleue” in France. The need for cross-border compatibility and the advent of the Euro led to many of these card networks being re-branded with the internationally recognised Maestro logo, which is part of the MasterCard brand. Some debit cards are dual branded with the logo of MasterCard as well as Maestro. The use of a debit card system allows operators to package their product more effectively while monitoring customer expenses.

2.2.1 Online Debit System

Online debit cards require electronic authorization of every transaction and the debits are reflected in the user's account immediately. The transaction may be additionally secured with the Personal Identification Number (PIN) authentication system; some online cards require such authentication for every transaction, essentially becoming enhanced ATM cards.

One complexity with using online debit cards is the requirement of an electronic authorization device at the Point of Sale (POS) and sometimes also a separate PINpad to enter the PIN, although this is becoming commonplace for all card transactions in many countries.

On the whole, the online debit card is generally viewed as better-quality to the offline debit card because of its more secure authentication system and live status, which alleviates problems with processing lag on transactions that may only issue online debit cards. Some online debit systems are using the normal authentication processes of Internet banking to provide real-time online debit transactions.

2.2.2 Offline Debit System

Offline debit cards have the logos of major credit cards, for example, Visa or MasterCard or major debit cards, for example, Maestro in the United Kingdom and are used at the point of sale like a credit card with payer's signature. This type of debit card may be subject to a daily limit, and/or a maximum limit equal to the current/checking account balance from which it draws funds. Transactions conducted with offline debit cards require 2 - 3 days to be cleared.

In some countries and with some banks and merchant service organizations, a "credit" or offline debit transaction is free of charge to the purchaser beyond the face value of the transaction, while a fee may be charged for a "debit" or online debit transaction, although it is often absorbed by the vendor. Online debit purchasers may also opt to withdraw cash on top of the amount of the debit purchase, if the merchant allows that transaction. Moreover, from the merchant's standpoint, the latter pays lower fees on online debit transaction as compared to "credit" (offline).

2.2.3 Electronic Purse Card System

Smart-card-based electronic purse systems, in which value is stored on the card chip, not in an externally recorded account, so that machines accepting the card need no network connectivity, are in use throughout Europe since the mid-1990s, most notably in Germany (Geldkarte), Austria (Quick Wertkarte), and France (Mon€o). In Austria and Germany, all current bank cards now include electronic purses.

2.2.4 Prepaid debit cards

Prepaid debit cards, also called reloadable debit cards, are used by a number of people. The prime market for prepaid cards includes *"unbanked people"*, a term used to describe various groups of individuals typically with poor credit ratings, who do not use banks or credit unions for their financial transactions.

The advantages of prepaid debit cards include being safer than carry cash, worldwide functionality due to Visa and MasterCard merchant acceptance, not having to worry about paying a credit card bill or going into debt, the ability for anyone over the age of 18 to apply and be accepted irrespective of credit quality and the ability to direct deposit pay checks and government benefits onto the card for free.

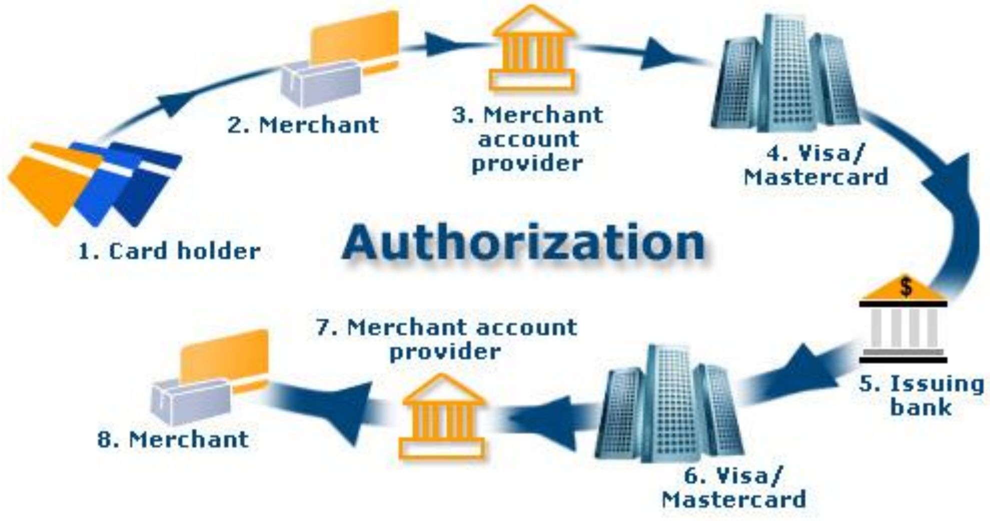
2.3 Credit Cards

Credit cards offer a lot of benefits to consumers, including the ability to afford expensive or cheap purchases, in good and bad times.

2.3.1 How do credit cards work?

Credit cards are issued by a credit card issuer, such as a bank or credit union, after an account has been approved by the credit provider, after which cardholders can use it to make purchases at merchants accepting that card. Merchants often advertise which cards they accept by displaying acceptance marks, usually derived from logos or may communicate this orally, as in "We accept MasterCard or Visa" or "We don't accept credit cards".

Below a brief description of how credit card processing works. Credit card processing has two parts:



Keep in mind this all takes ~2 seconds for an online transaction and about 15 seconds for a dialup transaction:

1. Cardholder presents the card (or the card number, expiration date and security code) to the merchant.

2. The Merchant communicates the card data to their Merchant Account Provider. They use either a credit card terminal, a POS system communicating over the internet or, in the case of an online transaction, a payment gateway, to communicate that data.

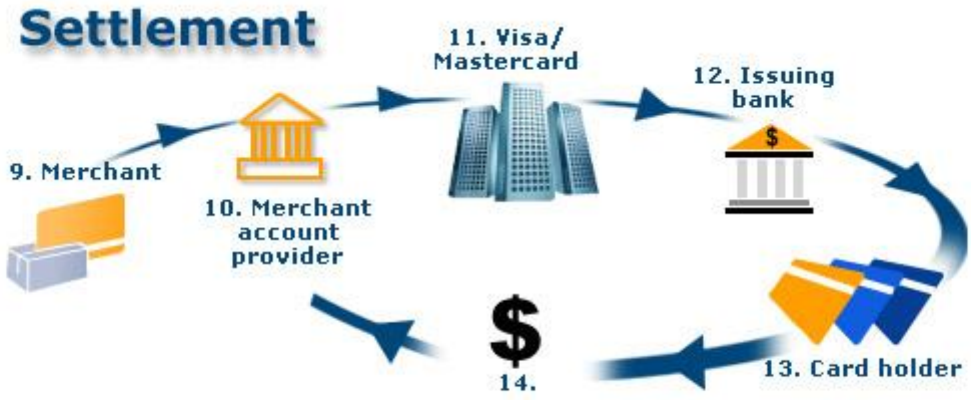
3. The Merchant Account Provider communicates the card information to the VISA or Mastercard network. Usually this is done via an intermediary, a larger Payment Processor.

4. Mastercard or VISA asks the cardholder's bank (these days usually a credit-card specialist) if the funds are available. If the funds are available, the transaction is authorized and the money placed on hold in the shopper's account (i.e. their available credit is reduced by the amount).

5. The issuing bank tells VISA / Mastercard what the result of the transaction was (either Authorized or Declined).

6. VISA / MC communicate the result back to the Merchant Account Provider

7-8. The Merchant gets the result and exchanges goods with the shopper.



9. At the end of the day the Merchant sends the day's "batch" of transactions to the Merchant Account Provider. If the merchant is using an Online Gateway or an IP-based terminal the batching is probably done automatically and is never really noticed by the merchant. If using an older dialup terminal the merchant probably has to hit a special button to initiate this process.

10-12. The merchant account provider sends the results to Visa / Mastercard.

13. The Issuing bank adds the amount to the cardholder's bill - the merchant no longer concerns themselves with the cardholder, unless there is a Chargeback or a Refund, because they will get paid no matter what. Collecting from the cardholder is the Issuing Bank's responsibility.

14. The Issuing bank transfers the money to the Merchant Account Provider, using an ACH (**Automated Clearing House**) transfer.

15. Your Merchant Account Provider deposits the proceeds into your business checking account using ACH.

Each month, the credit card user is sent a statement indicating the purchases made with the card, any outstanding fees, and the total amount owed.

The credit issuer charges interest on the amount owed if the balance is not paid in full typically at a much higher rate than most other forms of debt. In addition, if the credit card user fails to make at least the minimum payment by the due date, the issuer may impose a fine or penalty on the user. To help alleviate this, some financial institutions can arrange for automatic payments to be deducted from the user’s bank accounts, thus avoiding such penalties altogether as long as the cardholder has sufficient funds.

Many banks now also offer the option of electronic statements, either instead of or in addition to physical statements, which can be viewed at any time by the cardholder via the issuer’s online banking website. Notification of the availability of a new statement is generally sent to the cardholder’s email address. If the card issuer has chosen to allow it, the cardholder may have other options for payment besides a physical check, such as an electronic transfer of funds from a checking account. Depending on the issuer, the cardholder may also be able to make multiple payments during a single statement period, possibly enabling him or her to utilize the credit limit on the card several times over.

3.0 Security Issues and Solutions

3.1 Debit Cards

3.1.1 PIN Code and Signature

Debit cards are less secure because they can be used in two ways: with the PIN code or with a signature. The usage depends on the situation: when a person wants to withdraw funds from an ATM machine, he must use the PIN code, but when he is paying for goods at a merchant, he can choose between the two options. Whenever a person uses his debit card at a merchant, he should say that it is a credit card. Then, he will not have to enter his PIN code, his signature will be enough.

Using this method the bank will not charge the person for the transaction, but it will charge the merchant. Also, it there is proof that the person was in the shop, since the shop assistant has his signature on the receipt. Whenever it is possible, the owner should sign the receipt, because this is the only way the bank is able to trace in case of fraud that the debit card was used by its owner and not by another person.

3.1.2 Withdrawing cash from an ATM

There are other security issues concerned debit card usages. For instance, when a person wants to withdraw cash from an ATM machine, he should be very careful. He should never withdraw cash if he sees suspicious people around, and he should pay attention that nobody sees his PIN code. Also, it is very important to take the receipts; this is to make sure no one will see how much money is available or how much the person had withdrawn from the account.

3.1.3 Online Payments

Another security issue comes up when someone pays by debit card on the internet. One should never enter his card number in the required field unless he sees that the page is secure. This is shown either by a padlock on the lower right corner, or the address starts with “https” instead of the common “http”. These are the signs which show that a certain website is secure, otherwise the person has not proof the he had for the product he wanted. Another very important rule is to never give the card number through email or telephone, because it is not completely safe, a third party might have access to it.

The last safety measure is to keep track of the transactions. This can be done by keeping all the receipts, or by retrieving account information online, in case it is possible. This is the easiest way to notice if someone else has access to the owner's bank account. Another good method is to double check the monthly statements sent by the bank, and call if there are any suspect fees or charges.

3.2 Credit Cards

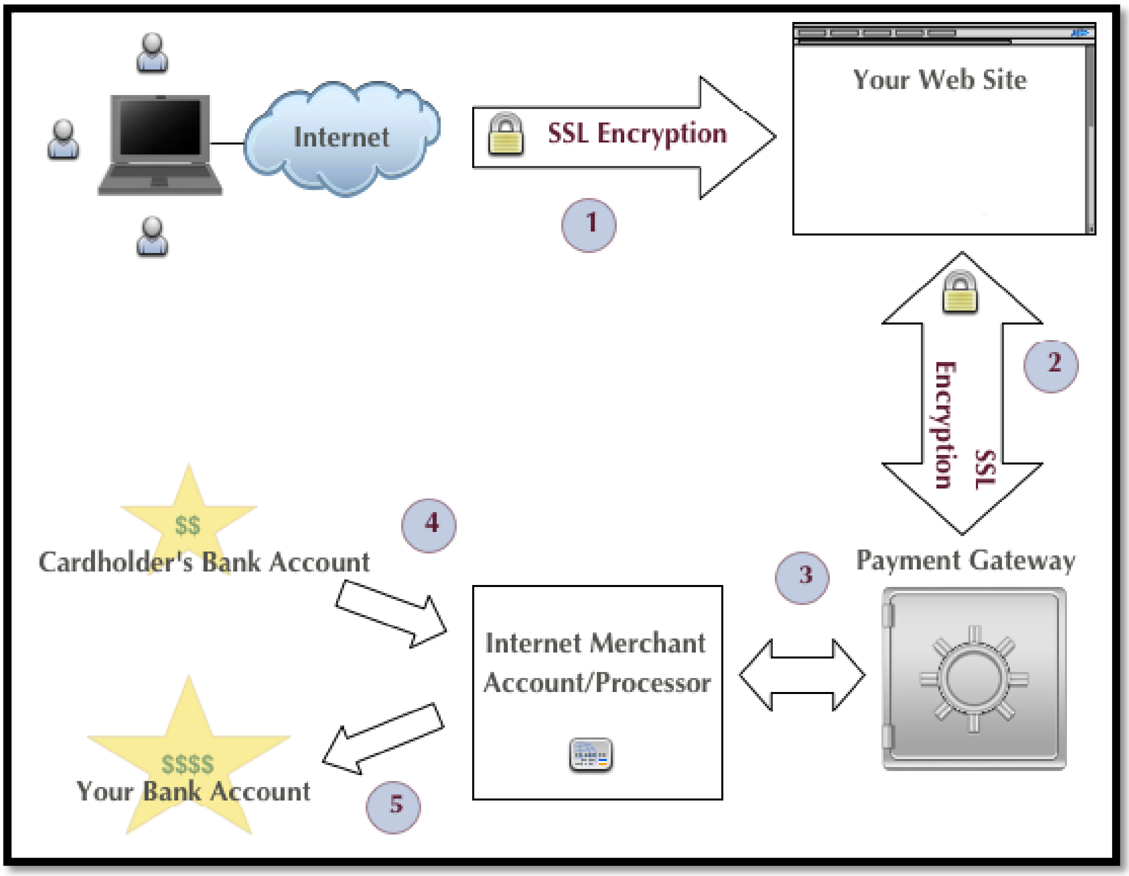
3.2.1 Physical Security and Privacy

Credit card security relies on the physical security of the plastic card as well as the privacy of the credit card number. Therefore, whenever a person other than the card owner has access to the card or its number, security is potentially compromised. Some time ago, merchants would often accept credit card numbers without additional verification for mail order purchases. It is now common practice to only ship to confirmed addresses as a security measure to minimise fraudulent purchases. Some merchants will accept a credit card number for in-store purchases, at which access to the number allows easy fraud, but many require the card itself to be present, and require a signature. A lost or stolen card can be cancelled, and if this is done quickly, it will greatly limit the fraud that can happen in this manner. European banks can require a cardholder's security PIN for in-person purchases with the card.

3.2.2 Internet Fraud

Internet fraud may be by claiming a chargeback which is not justified, or carried out by the use of credit card information which can be stolen in numerous ways, the simplest being copying information from retailers, either online or offline. Despite efforts to improve security for remote purchases using credit cards, security breaches are usually the result of poor practice by merchants. For example, a website that safely uses SSL to encrypt card data from a client may then email the data, unencrypted, from the web server to the merchant; or the merchant may store unencrypted details in a way that allows them to be accessed over the Internet or by a rogue employee; unencrypted card details are always a security risk.

The diagram below illustrates a secure online transaction using Secure Socket Layer (SSL) Encryption.



The **PCI DSS** is the security standard issued by The PCI SSC (Payment Card Industry Security Standards Council). This data security standard is used by acquiring banks to impose cardholder data security measures upon their merchants.

Controlled Payment Numbers used by numerous banks such as Citibank (Virtual Account Numbers), are another option for protecting against credit card fraud. These are generally one-time use numbers that front one's actual account (debit/credit) number, and are generated as one shop online. They can be valid for a relatively short time, for the actual amount of the purchase, or for a price limit set by the user. Their use can be limited to one merchant. If the number given to the merchant is compromised, it will be rejected if an attempt is made to use it again.

A similar system of controls can be used on physical cards. Technology provides the option for banks to support many other controls too that can be turned on and off and varied by the credit card owner in real time as circumstances change (i.e., they can change temporal, numerical, geographical and many other parameters on their primary and subsidiary cards). Apart from the obvious benefits of such controls, from a security perspective this means that a customer can have a "Chip and PIN" card secured for the real world, and limited for use in the home country.

3.2.3 Theft

In the event of a theft, the thief will be prevented from using the cards in countries that do not support the "Chip and PIN" EMV (Europay, MasterCard and VISA). Similarly, the real card can be restricted from use online so that stolen details will be declined if it is used by an unauthorized user. Then when card users shop online they can use virtual account numbers. In both circumstances an alert system can be built in notifying a user that a fraudulent attempt has been made which breaches their parameters, and can provide data on this in real time. This is the optimal method of security for credit cards, as it provides very high levels of security, control and awareness in the real and virtual world.

3.2.4 Counterfeiting

There are security features present on the physical card itself in order to prevent counterfeiting. For example, most modern credit cards have a watermark that will fluoresce under ultraviolet light. A Visa card has a letter "V" superimposed over the regular Visa logo and a Mastercard has the letters "MC" across the front of the card. Older Visa cards have a bald eagle or dove across the front. In the aforementioned cases, the security features are only visible under ultraviolet light and are invisible in normal light.

4.0 Conclusion

All in all, credit cards are a lot safer than debit cards, because banks offer lots of extra features and advantages to credit card owners. Also, it is less likely to come across credit card fraud, and even if it happens, banks offer assistance and the owner will surely get his money back. As a last conclusion, while debit cards bring serious money to banks, people should use them as credit cards and always sign the receipt; this will help them a lot in case of fraud.

5.0 References

- Creditcardsquote: **http://www.creditcardsquote.info**
- Wikipedia: **http://en.wikipedia.org**
- Federal Deposit Insurance Corporation: **http://www.fdic.gov**
- WiseGeek: **http://www.wisegeek.com**
- AdvancePro: **http://www.advanceware.net**
- Oasis: **https://www.oasis-open.org**

Appendix A

List of Acronyms

ATM	Automatic Teller Machine
CNP	Card Not Present
EFTPOS	Electronic Funds Tranfer at Point of Sale
EMV	Europay, MasterCard and VISA
PCI DSS	Payment Card Industry Data Security Standards
PCI SSC	Payment Card Industry Security Standards Council
PIN	Personal Identification Number
POS	Point of Sale