REF.NO:-DPO/DEC/7

IN THE MATTER OF:-

Complainant

VERSUS

Respondent No. 1
Respondent No. 2

A complaint was lodged on 7 June 2011 at the Data Protection Office under section 11 of the Data Protection Act against respondents nos. 1 and 2 for storing debit/credit card details during purchase transaction at Point of Sale (POS). Complainant has shown the investigation unit of the Data Protection Office (DPO) his debit card which he has used to pay at the POS. He has also submitted a copy of respondents' Nos. 1 and 2 receipts where the debit/credit card number has been recorded.

According to complainant, the bank debit/credit card details which are stored at the respondents' site can later be used for illicit payment if hackers break the hypermarket servers. Complainant alleged that a fraud can occur if someone throws the customer receipt together with the bank receipt or if they are stolen. The customer or till receipt contains the bank account number and the bank receipt contains the name of the customer with truncated account number.

If the expiry date and name of the credit card holder are printed in the bank's payment receipt this can lead to the commission of a fraud when captured by a hacker or cracker. These details can be used to generate the correct pin code by trial and error or make use of the brute force attack during any internet shopping transaction provided that the expiry date has been inserted by trial and error, as alleged by complainant. Complainant is thus alleging that there exists a risk that if his card details are stolen during their storage at point of sale, this may potentially result in an illicit transaction taking place on his bank account.

On 3 March 2011, complainant sent a letter to the General Manager of Respondent No. 1 and the CEO of Respondent No. 2 regarding the above complaint. Complainant has also sent a copy of the complaint letter to the Prime Minister's Office (Defence and Home Affairs Department) which was channelled to Data Protection Office (DPO) on 1 April 2011.

The Investigation Unit of the DPO have investigated the matter and requested the necessary advice from (...) and (...) about any alleged potential risk involved in keeping the debit card number's details at the respondents' site.

The (...) has confirmed that all relevant data is transmitted in a secure environment and is compliant with international standards of the Card Associations, as follows:-

- **No credit card numbers are printed on the receipt of merchants;**
- **(...) uses the "masked card technique" on cards which hides the card number and expiry date on receipt, during a transaction;**
- **Card numbers are not stored on the (...) POS terminal, thus preventing merchants from having any access to same;**
- **All (...) POS have been configured according to Payment Card Industry Data Security Standard (PCIDSS), thus preventing any retrieval of card information; and**
- **All (...) cards are 'chip'- enabled and hence provides greater security and comfort to the cardholder in compliance with the best of breed world standards for card safety. The chip enabled technology offers the highest level of payment security requiring PIN authentication at POS and cash dispensers.**

Thus, card details are not stored on (...) Point of Sale (POS) and the added security feature of truncating the 16 digit card numbers printed in customer and merchant receipts gives sufficient protection to the cardholder's personal details. Furthermore, (...) merchants are bound by an agreement with (...) whereby they are not allowed under any circumstances to sell, purchase, provide or otherwise disclose cardholder's account information or personal information to anyone except the Bank. The (...) has further stated being in compliance with data protection standards.

The (...) report stated that they have never given any instruction to merchants for bank details to be recorded in receipts at any POS. It has also been their contention that stealing visible card details cannot by itself lead to illicit operations taking place on concerned bank accounts whereas once the electronically stored data of the magnetic strip or chip card is stolen, then the possibility for organised pillage of card accounts occuring can become reality. According to (...), this is rare although it has occurred worldwide and is being fought against all over the world and especially by the card companies such as VISA, MasterCard, Amex, amongst others whose credibility as service providers are crucially at stake in this particular type of situation and are committed to find solutions to protect the personal financial information of the cardholder.

The representative of respondent no.1 has stated that the company has changed its internal system so that tills' slips do not show the full card numbers. This compliance revision was finalised in July 2011 and all issues attendant to non-compliance were addressed.

In relation to the card details, it was highlighted by respondent no.1 that collecting and processing payment card information is a legal activity, undertaken by retailers internationally in order to process payments and facilitate response to queries and/or questions regarding transactions between the banks and retailers. It was also confirmed that it does not store further personally identifiable information (such as name and/or address) together with the payment card number or additional details such as CVV (Card Verification Value). It was however conceded that printing the full number on the till slip was problematic and as such it is now ensuring that this situation is remedied and addressed in accordance with the compliance program that it undertook.

In relation to the security of data kept, the data is stored in a secured location and payment numbers are masked (so that full number is not visible) or encrypted. The data is further subject to an audit to ensure that the information remains securely kept. Points of sales are additionally being rectified to ensure that the numbers are marked at all points. Copies of receipts dated 04 August 2011 and 10 August 2011 were given as proof of the changes made on the till receipts. The receipts contain the cardholder debit card number and the bank counter receipt contains cardholder name whereas the expiry date is encrypted as 'XXXX'.

Respondent no. 1 has now masked the middle numbers with the exception of the first 6 numbers which represents the bin number and the last four numbers on the till slips and the system further ensures that nobody has access to the client's confidential information. The reason for not masking the first 6 number is to determine what type of card the client has in the event of enquiries. The representative of respondent no.1 also stated that previously they were keeping the debit cards' numbers in order to keep track of the customers more particularly to deal with refund of funds when a customer returns goods purchased. Though respondent no.1 was recording the 12 digits of the card number, investigation revealed that there was no such risk involved to hackers as debit card cannot be used to do internet payment. Respondent no. 1 is also aiming to be one of the first level 1 retailers to reach the milestone 1 level for PCI compliance.

As indicated above, the practice of printing out the full number was historically attended to in order to facilitate queries and interaction with the banks by respondent no. 1. It is mindful of the risk involved and, as such, has addressed this issue to ensure the utmost safety and diligence with the information of our customers. Respondent no. 1 has assured the investigation unit of its best effort to rectify this situation in a manner which should provide the necessary comfort to their clients.

Investigation reveals that respondent no.1 has already taken corrective measures in order to skip recording any card holder number.

The Investigation Unit scheduled a site visit on 9th December 2011 at respondent no. 1 premises with his representative to verify and ensure that corrective measures have been

implemented. Respondent 1 showed them 2 random customers who effected payment with debit cards.

The receipt of respondent no.1 did not contain any cardholder debit card number and the bank counter receipt contained only the last cardholder name whereas the expiry date is encrypted as 'XXXX'.

However, it was found that (...) POS credit card receipt (kept at respondent no.1 premises) contains the full credit card number of the customer but without the cardholder's name and without any CVV.

Thus, respondent no.1 no longer keeps any card holder's name nor any three digits CVV at the POS for a valid payment transaction to be effected. Respondent 1 has also replied that there has not been any reported case to it concerning the occurrence of any such type of fraud.

The (...) was contacted to provide clarifications as to why credit cards' numbers are stored in the receipt of the merchant's POS during the transaction. Up to now, the DPO has not received any response from the (...) concerning credit card details kept at POS.

A meeting was arranged at DPO on 10 August 2011 with the representatives of respondent no. 2. A second meeting was held on 6 December 2011 with the representative to provide further clarifications and submit his declaration or explanation as soon as possible. Respondent No.2 has stated that it sells its products and services at its various points of sales throughout the island, for which payment is accepted by cash or debit/credit cards. It keeps certain details of the debit/credit card to keep track of the payment made by the customer and for reconciliation purposes with the bank. The last 4 or 6 digits of the debit/credit card are kept in the billing system for this purpose. The initial numbers are either blanked or masked by using dots or crosses. It does not keep other details of the debit/credit card. It also ensures that only the last 4 or 6 digits of the debit/credit card are displayed in the receipt. The billing or customer management system is for internal use by its employees and are secured against hackers through firewalls. Access to the system is through such authentication means as user name and password. It is worth noting that all its staff are governed by an oath of secrecy and are fully aware of the provisions of the Data Protection Act regarding confidentiality and security of personal data being collected and processed.

The Investigators then moved at respondent's no. 2 site on 15th December 2011 to verify the situation. They requested respondent no. 2 to show them the debit/credit card receipt together with the receipt of the customer in order to verify the card number's details found in the receipts. All the receipts contained only a six digit number which cannot be used to carry out any illicit transaction.

The Investigators further enquired with respondent no. 2 as to why full card details have appeared on the receipt of complainant. The Executive Regulatory Compliance of

respondent no. 2 replied that the company does not keep card details on receipts but that complainant's reported case has occurred as a result of technical problems encountered with the system. Respondent no. 2 ensures that such occurrences now do not happen as daily verifications are carried out.

The investigation has also revealed that the details of the debit card can be kept at the respondents' place provided there is a reasonable justification for so doing or a specific purpose in compliance with PCIDSS (Payment Card Industry Data Security Standards) and data protection principles.

Furthermore, investigation has revealed that Internet payment is only done by Credit Card which requires a 3 digit numbers Credit Card Verification Value (CVV) authentication and is located at the back of the card and is used as the credential of the credit card. The Credit Card number itself is not enough for a credit card transaction as the full name of the card holder together with its expiry date is required for any internet transaction to be effective. However, brute force attack can be applied to obtain the CVV provided that the card holder name as well as the Credit Card Expiry date of the credit card is recorded.

Both respondents were contacted during the enquiry and sections 22, 23, 24, 26 and 27 of the Data Protection Act were clearly explained to them.

Complainant was contacted again on 17th March 2012 to provide additional information whether any illicit transaction on his bank account has taken place. Complainant replied that he has not noticed any illicit transaction on his bank account up to now. He has further given a written declaration on 10 May 2012 that he is satisfied by the investigation carried out by the Data Protection Office.

The Data Protection Commissioner has decided as follows:-

It has been proven beyond reasonable doubt that respondents Nos. 1&2 have displayed the required efforts to remedy the potential dangers to personal information of customers being used for illegal transactions by adopting appropriate security and organisational measures such as adopting a compliance and security program to safeguard the collection and processing of all personal data belonging to customers.

All collection of personal information are subject to a lawful and necessary purpose. Debit/credit cardholders should be informed about the different uses to which their information are subjected to, and the intended recipients of these information as well, by respective banking institutions and other relevant parties, in compliance with section 22 of the Data Protection Act (DPA). Express consent of the owner of the information (the debit/credit card holder) may be required where exceptions do not apply under section 24 of the DPA. All appropriate security and organisational measures to prevent any potential harm to the financial information involved should be taken, where this has not already been effected by all respective parties to protect personal data of customers.

However, (...) is required to show compliance with international and local standards by ensuring that personal information as identified above are not kept illegally, in contravention with our laws or without reasonable justification. Failure to show compliance may result in prosecution undertaken by this office.

Mrs Drudeisha Madhub

Data Protection Commissioner

Data Protection Office

Prime Minister's Office

4th floor, Emmanuel Anquetil Building,

Port Louis

14.05.12