

TOMORROW >> India Diary
Numbering Indians
proving an uphill task



FOCUS

How safe is your credit card?

The seizure of cloned foreign credit cards, including 70 blank ones, during a raid in a house in Alor Setar recently may be a cause for concern but industry experts say since the implementation of the chip-based cards, it is more difficult for fraud to occur now.

By **RASHVINJEET S. BEDI**
sunday@thestar.com.my

It was a routine credit card transaction for travel agent Yong Lee Heng (not his real name). After getting clearance from the credit card's issuing bank for a payment of RM17,000, Yong processed the airline tickets for five African men.

But 26 days after the transaction, the bank called Yong to tell him that the credit card that had been used was forged. The bank then retrieved RM6,000 from his credit account and demanded that he pay the remaining RM11,000.

Yong insists it was unfair to make him pay for a transaction that the bank had approved.

"We are just a travel agency. How would we know if a card was forged?" an agitated Yong argues.

He says the bank is now prepared to offer him a discount and payment by instalment but Yong is having none of that.

His case is just one instance of credit card fraud that is still happening in the country, although it is occurring on a lesser scale now.

According to statistics from Bank Negara, the total amount of credit card fraud in 2004 was around RM68mil. This fell to around RM20mil in 2006, when use of the chip-based cards using Europay-MasterCard-Visa (EMV) standards was implemented.

A Commercial Crimes Investigation Department (CCID) spokesperson says that while credit card fraud is not as severe as before, it is still considered a problem.

Recently, the Kedah CCID seized 137 cloned foreign credit cards, including 70 blank ones, during a raid in a house in Alor Setar. The cards are those cloned from non-EMV cards.

"Cards using magnetic strips are much easier to forge than the chip-based ones," says the CCID spokesperson.

But the EMV measures have not stopped the still-active syndicates who have come up with new ways of committing fraud (see accompanying story on the *modus operandi* of credit card fraud syndicates), says the spokesperson.

These include the Card Not Present (CNP), Account Take Over (ATO), false application, replacement of original credit card with another card and the classic case of stealing other people's cards and using them.

According to Bank Negara, the CNP transactions and unauthorised transactions using lost and stolen credit cards remain the main source of fraud losses, accounting for 57% and 20% of total credit card fraud losses respectively in 2009.

MCA Public Services and Complaints Bureau head Datuk Michael Chong says his office is still receiving complaints of credit card fraud cases. In 2008, the department received 14 reports involving RM76,000; in 2009 it was 13 cases involving RM45,000. So far this year, the department



Easy access: A frequent complaint by consumer groups is the fact that banks pre-approve credit cards and send them to customers who did not sign up for them in the first place.

has received five complaints involving RM63,000.

One of the cases involved someone who was in jail when the application for the card was made.

"This is such a big joke. How was his card approved when he was serving his sentence? Banks have to be more stringent in their approval process for credit cards," Chong says.

He believes banks are fighting for business and might be approving credit cards easily.

A frequent complaint by consumer groups is the fact that banks pre-approve credit cards and send them to customers who did not sign up for them in the first place.

"If credit cards are important, then the banks must make sure the new cardholders collect them personally instead of sending them by mail," says Chong.

There have also been cases where personal details and signatures of those applying for one credit card have been reused to apply for others.

Chong also highlights incidents where credit cards can be switched, citing the case of a woman whose car was broken into while she was out jogging. As her purse was not stolen, she did not think there was anything to worry about.

Later, Chong relates, the woman

»This is such a big joke. How was his card approved when he was serving his sentence«



DATUK MICHAEL CHONG

received a call from her bank requesting her to verify some transactions she was supposed to have made.

When told she had spent RM24,000, she checked her purse and found her credit cards had been replaced with similar looking cards.

Consumers are now protected if they are victims of credit card fraud, according to the Consumers Association of Penang (CAP). Its president S.M. Mohd Idris says that in 2003, Bank Negara came up with a credit card guideline and clause (13.2) that

Many ways to trick cardholders

The Commercial Crimes Investigations Department (CCID) says credit card fraud can occur in several ways.

1. ATO (Account Take Over)

Police believe that insiders provide details of credit cards to the syndicates. Members of these syndicates then contact the "card centre", reporting that the cards are lost and that they are the rightful owners. They then request a change of address. Banks post the replacement cards to the new address.

2. CNP (Card Not Present)

Using other people's credit card account numbers to purchase goods or services (such as air flight tickets or reserving hotel rooms) via the Internet. The credit card account numbers and the CW/CVC numbers are obtained through cashiers in shopping complexes, hotels and other commercial areas.

3. False Application

Applications are made by falsifying identity card numbers, pay slips and employer certification letters. Syndicates use unoccupied premises as the address for correspondence.

4. Stealing other people's cards and using them

There are cases where credit cards are stolen and used in many places especially fuel stations.

5. Replacement of original credit cards with another card

When the customer pays with a credit card, the cashier will return a similar looking card to him or her. The customer only finds out that the card has been switched when he receives the credit statement with purchases he has not made included in it.

says banks cannot charge the cardholder more than RM250 for fraudulent transactions if the cardholder is not a party to the fraud and the loss of the card was reported as soon as possible.

The clause says that where the amount in dispute is more than RM250, then the onus is on the bank to prove that the cardholder has acted fraudulently or failed to inform the banks as soon as reasonably practicable upon discovery of the loss.

> TURN TO PAGE 19

Upgraded security features reduce risk

> FROM PAGE 18

"In reality, the cardholder has to try to prove that the transactions were not done by him. Even then the bank will say he is responsible for all transactions carried out before the loss is reported to the bank," says Idris.

In June 2009, the KL High Court judge held that the Bank Negara guideline "had the force of law" and that the guideline limited the liability of the cardholder to only RM250 where loss is reported promptly.

Idris says that before the High Court ruling, cardholders ended up paying more than the RM250.

Even big businesses are victims of credit card fraud.

Johan Aris Ibrahim, head of Financial Services and Loyalty, AirAsia, says that although credit card fraud is on a low side (below 1%) compared to the size of its business, they are continuously aiming for zero fraud.

He says that since 80% of AirAsia's revenue is derived from Internet bookings, the management places high importance to keeping credit card fraud transactions at a minimum.

Johan says the company has a Credit Card Fraud Control Unit (CCFCU) operating 24/7 to detect fraudulent credit card transactions and they liaise closely with all the banks in Malaysia to verify suspicious transactions.

AirAsia, meanwhile, is encouraging their cardholders to activate the 3-D Secure feature on their credit cards with their respective banks. Johan explains that once activated, the bank will text the card holder the 3-D Secure pin. Cardholders will then be requested to input their 3-D Secure pin for every online transaction.

"This will prevent fraudulent credit card transactions in case the credit card gets stolen," says Johan.

However, according to research house Lafferty Group, payment card fraud and attempted fraud rates in Malaysia have

dropped substantially following the migration from magnetic stripe to chip-based ATM cards and EMV standards on credit cards as well as the introduction of additional security measures for Internet banking.

"Cloning is a far less serious issue than before the adoption of EMV," says Andrew Neeson, who heads the Cards and Payments and Consumer Finance Research section at Lafferty Group.

Despite this, says Neeson, combating fraud and financial crime is an unrelenting battle for the global retail banking and cards and payments industry as fraudsters will always attack what they perceive to be the weakest area of defence.

"Phishing attacks are a major issue in credit card fraud as they enable criminals to fraudulently acquire consumers' user names, passwords and credit card details. Phishers have expanded their reach to web infrastructure sites such as domain registrars and hosting services," he says.

He adds that banks and payment networks are fighting back against fraud with the two-factor authentication process.

For example, Visa Europe has announced that its Visa CodeSure online payment initiative is now fully available for commercial launch after a number of consumer pilots and rigorous testing with European banks.

Neeson says the Visa CodeSure system improves online security by providing a Visa card with an alpha-numeric display and 12-button keypad and battery that is embedded in the card.

"The payment network explains that as cardholders are required to enter their PIN for every online transaction, the CodeSure card will prevent any unauthorised use," he says.

He adds that MasterCard Europe has also unveiled a debit card with a built-in display window and touch-sensitive button that can provide cardholders with information, such as a dynamic passcode and account balance.

Tips to minimise being a victim of credit card fraud

1. When out and about, never let your cards out of your sight.
2. Check your bank statements thoroughly to ensure there are no suspicious transactions.
3. Sign up to Verified by Visa® or MasterCard® SecureCode™. This will put a stop to most unauthorised online spending.
4. Don't let restaurant or shop staff take your credit card out of your sight when you are paying.
5. Shred any documents, statements or receipts that contain personal financial information. A clever fraudster can do a lot of damage with just a credit card receipt.
6. Don't let anyone else take money out on your behalf. Never write down your PIN, passwords or user names.
7. When entering your PIN at a cash machine (ATM), cover the keypad with your spare hand to protect it from prying eyes or hidden cameras.
8. Sign any new card as soon as they arrive.
9. When discarding expired cards, cut them up, making sure you cut through the magnetic strip and the chip.
10. Keep track of your card expiry dates. If a replacement card hasn't arrived by the time your old one expires, call your bank or card issuer to check whether a new one has been sent out.
11. Be careful when giving out personal information in a website, e-mail, instant messaging systems, chat rooms or on message boards, especially when you are not sure. You have the right to ask why and how the information is to be used.
12. Read privacy statements.
13. Close compromised credit card accounts immediately.
14. Monitor your credit card statements. Keep in mind that fraudulent activity may not show up right away.
15. Consult your financial institution about any unusual activities on your accounts.
16. Watch for signs of identity theft: late or missing bills, receiving credit cards that you didn't apply for, being denied credit or offered less favourable terms for no apparent reason, or getting contacted by debt collectors or others about purchases you didn't make.



Source: Card Protection Plan Limited (cppasia.com) and Cybersafe Malaysia

GRAPHICS © 2010