

Credit card issuers generally lose about \$1.5 to \$2 billion every year because of the frauds, most of the times committed by insiders in organizations. This scenario has thrown yet another challenge to the professionals. All CAs serving big firms as auditors, consultants, managers, etc. need to guide internal audit departments to not only handle such 'fraud situations' but also avoid them. This article provides an overview of the frauds and the ways to detect them.



Credit Card Fraud: Causes & Cures

from professional's perspective

London Police smashed a 5 million pounds credit card racket on 27th of October 2004 that involved Royal Mail workers. The credit cards received by the Department were sold by sorting office staff to unscrupulous elements outside on bribe and these were subsequently sold off to innocent people at a relatively small price.

Such cases are increasing worldwide and India is no exception. The culprit are not only the outsiders but insider fraudsters too who cheat their organization to make quick buck.

Credit card fraud has been defined by 'The Fraud Examiners Manual' as "the misuse of a credit card to make purchases without authorization or counterfeiting a credit card". 80% of the US households have at least one credit card. And this situation is fast catching up in India too.

Every competition driven bank in India is under pressure to issue more cards. More than nine million cards were in circulation in India by the end of December 2003. In 2004 it is estimated to have touched 15-20 million mark that includes debit cards too. As income from interest has considerably reduced due to reeducated rates, banks try to fix a minimum target of



—Sree Jagadeesh

credit card issue. Naturally, the chances of frauds also go up.

Bank credit card issuers lose about \$1.5 to \$2 billion every year because of fraud. The Visa and master card, the two largest credit card issuers lose most. Generally the Credit card fraud is committed successfully on most of the occasions. Chances of being caught are small

and the necessary legal procedure to book the culprit based on strong evidences is not available.

MAJOR TYPES OF FRAUDS

1. **Unauthorized use of credit cards:** This is the most frequent type of

fraud. Fraudsters use the lost card or stolen cards within hours of the loss or theft. On many occasions, the cardholders are not aware that their cards are stolen or lost, until they get their monthly statements. Many cardholders do not sign on the back of the card also, which makes the fraud an easier job.



The author is a member of the Institute working as Manager, Internal & Control in Video Home & Electronic Centre, Doha (Qatar). He can be reached at jagadeesh@jumboqatar.com

2. **Online credit card frauds:** As per information available with Fraud Examiners Manual, more than \$700 million in online business was lost to fraud in the year 2001. In general about 5% of the total sales made on line were fraudulent. Now, security/authorization levels are available to prevent this type of fraud but many cardholders are still unaware of these security systems available in the Net.
3. **Fraud groups:** There are some organized groups which steal credit card and bank information of card holders from net and the credit cards are duplicated for distribution among the group. They prepare false ID cards also for producing at the counter in case of identity check. Then these groups go on a spending spree till the limit is over.



4. **Shave & paste:** Any number of alpha or numeric characters are sliced from the card and other characters are attached to the card surface utilizing fast drying epoxy-type glues. This is done to put an entirely new but valid account number or to change the name, so that the fraudster can use the card as if it is his own.
5. **Counterfeiting the cards:** This is one of the common methods used by some organized groups. However, duplication is done in a very scientific way and the counterfeit card appears to be genuine. The most difficult part of duplication is to produce the hologram. However, true hologram use a “lenticular refraction” whereas the duplicate is only a reflected material. Duplicate holograms are attached on the surface of the cards, whereas the original is embossed. Duplicate holograms some times will not change colours as the original ones do when viewed from different angles. Even these holograms are duplicated and distributed for

a prize. This method is very common in China, Taiwan and Hong Kong.

6. **Mail order fraud:** In many cases, the fraudster would act as a Credit card representative and then informs that a Prize or Discounted travel trip has been won by the card holder. The victim is asked to read out the credit card number for verification. Many cardholders fall victim to this tactics. This card number is used to purchase a lot of material through Catalogues and mail orders. The fraudster would give an address not occupied by him, and then later collect the material from the parcel service offices.

INSIDER FRAUDS

Many banks issue credit cards to the employees of companies and trading establishments on the basis of Salary Slip or Certificates. This may lead formation of an inside fraud ring or group to misuse the cards and cheat the establishments.

In many companies and trading concerns, the employees are offered the products at discounted rates. Employees buy these items using credit cards and then sell to outsiders at normal selling price, thus making themselves a profit in the process. Some times this happens without any authorization and management fails to detect the use of cards of their own employees.

In trading establishments such as Electronic shops, home appliances, textile shops or fancy/gift articles shops, these types of frauds are common. This is done in an organized manner with the collusion of the show room in charge. At the time of “Discount Sale Campaign”, these groups use their credit cards to “purchase” the items at a much-discounted rate. These are subsequently sold to outsiders, usually friends at a normal rate.

Sometimes the Cash Sales are converted in to Card Sales. After receiving the cash, the invoice is converted in to credit card sales, using one of the employees card. Cash is then rotated for the credit period. This may also happen when the customers happen to be friends of the employees.

This type of fraud will not come to the notice of the management, till it actually scrutinizes the credit card sales. Even if found, the staff can very well say that this is “sold” to him or to his friend which is a genuine transaction. The legal formalities to punish such frauds are not adequate at present.

PREVENTION & DETECTION

At point of sales:

- ◆ Check for the signature. If there is any doubt ask for an ID card.
- ◆ If the customer is too young and purchasing large volume of goods, then the staff should be careful to check the genuineness of the card.
- ◆ Check the hologram and logo, if they are blurred or tampered.
- ◆ All visa cards should have CV, BV or PV printed next to expiration date.
- ◆ All visa cards should have their BIN (four digit) printed above the first four digits of the printed account number, if they are missing or not matching, then the cards are counterfeited.
- ◆ A large 'MC' is visible under UV lights for Master cards.
- ◆ In case of AMEX cards, a duplicate number is on the reverse of the card to ensure the card number appearing in the front has been altered.

At institutional level

- All card issuers like VISA, MASTER and AMEX

have their own unique features to prevent the fraud or misuse of the credit cards.

- SMART CARDS – these cards contain a micro-processor memory chip instead of holograms. These cards are able to identify the user through encrypted information on the chip and must be inserted in to a 'card reader' attached to the computer. That means the card cannot be used by unless the purchaser is currently holding it. This allows cardholders more purchasing options as well as increased security. These cards are becoming popular in most of the countries.
- Computer edits – Computer edits are inbuilt in some cards, so that the user is fixed a limit in terms of number of times the cards is used or the amount of money spent in a particular month.
- PIN number – this is one of the best methods to prevent unauthorized use of the card. It is usually difficult to find out the PIN numbers.

As long as credit cards are in existence, the related credit card frauds are bound to happen. Many fall prey to the fraud. The issuers look for newer methods to prevent such frauds. It is in their own interest that the cardholders should keep their cards safely and use the cards wisely to protect themselves from frauds. ■

ROLE OF AUDITORS

- ✎ External auditors should advise their clients to train the staffs who are handling the credit card sales.
- ✎ The concerned staff should be able to check the signature and should be able to distinguish a counterfeit card from a genuine card.
- ✎ Proper training should be given to the staff to check signature, check the hologram (which is three dimensional), check the BIN of the card. BIN must be preprinted above the embossed number. If these numbers do not match exactly, the card has been altered or counterfeited.
- ✎ If there are "ghost images" of the numbers, behind the embossing on either the front or the back of the card, it has been re-embossed.
- ✎ Check the ID cards, if the cardholder seems to be nervous, too young and make expensive purchases.
- ✎ Role of Internal Auditors are very high when the fraud takes place inside the organization itself. The only way to prevent this is to check the credit card transactions on a monthly basis and note down the purchases, if any, made by the employees.
- ✎ Look for the authorization for discounts and make sure that the purchases are for the employees own use and not otherwise.
- ✎ Frequent use of credit card of employees to be analyzed often.
- ✎ Formulate policies in respect of purchases by the employees using credit cards with respect to the value, frequency and authorization etc.