Card Fraud Debit & Credit Card

Mohammad Tohidur Rahman Bhuiyan

A credit/debit card (or, any kinds of electronic payments card) is a convenient method of payment and it has become a way of life in many parts of the world including our country, Bangladesh. Today, use of cards/ plastic money is preferred than to use hard cash. All cards have one thing in common, namely that the bearer can obtain something of value simply by presenting the card.

Fraudulent transactions attempted on legitimate credit card accounts have risen sharply in recent years. While in some instances, credit card fraud occurs when someone's physical credit card is lost or stolen by another party who uses it, credit card fraud is driven primarily by compromise of credit card account data during their normal course of usage. Such compromises can range from theft of data by skimming (copying) the information contained on a small number of credit cards' magnetic stripes to large scale data breaches where millions of credit card accounts are compromised through exploitation of a data security weakness at an online or physical store or chain. Stolen credit card data is then often used to attempt fraudulent online purchases. Technological advances have allowed the perpetrators to produce counterfeit cards with stolen data that resemble the genuine card so closely that it is difficult for shopkeepers, tellers, police and bank investigators to identify a fraudulent card. Identity theft and the exponential growth of the internet have further compounded the crime of credit card fraud by allowing for on-line purchasing, resulting in huge financial losses to the card industry, banks and consumers alike.

This article discusses credit card fraud, key types of card fraud and offers potential information about the measures be taken to reduce it.

Some of the Credit Card Fraud Attacks

Between July 2005 and mid-January 2007, a breach of systems at TJX Companies exposed data from more than 45.6 million credit cards.

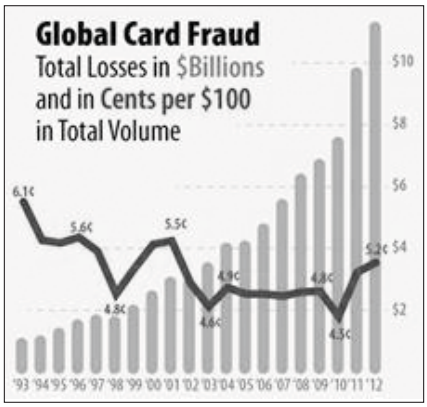
In August 2009, same man behind the TJX Company fraud was also indicted for the biggest known credit card theft to date — information from more than 130 million credit and debit cards was stolen at 'Heartland Payment Systems', retailers '7-Eleven' and 'Hannaford Brothers', and two other unidentified companies.

On September 8, 2014, The "Home Depot, USA" confirmed that their payment systems were compromised. They later released a statement saying that the hackers obtained a total of 56 million credit card numbers as a result of the breach.

Types of Card Fraud

Card not present transaction fraud
Identity theft (Application fraud)
Card Skimming
Tele phishing
Balance transfer checks

Card Not Present Transaction fraud: Since card-not-present transactions eliminate the situation where both the owner and the card are present, exposure to fraud increases by stolen information.



Identity theft: It happens when a criminal obtains your personal information — such as your full name, Social Security number, date of birth and address by any means. Once the criminal has obtained your personal information, he or she can commit identity theft by taking control of your existing credit accounts or opening new ones. Some people refer to this as 'identity fraud.'

Card Skimming *or* ***card cloning:*** It uses a Card Skimming device to fraudulently copy bank customer details stored on the magnetic strip (brown/black strip at the back) on a debit or credit card. Whenever you present your card for payment you run the risk of being skimmed. However, the majority of skimming incidents in South Africa are recorded around ATMs and, to a lesser extent, at retail merchants when bank cards are presented for payments. The customer and card information stolen with skimming devices is often used to manufacture counterfeit (duplicate) cards which criminals use to make fraudulent transactions on a victim's account.

Tele Phishing: Tel phishing is another way thieves try to collect sensitive information from you. In this type of fraud, they will either contact you by telephone or send you a fake e-mail and ask for you to respond by telephone.

Balance transfer checks: Some promotional offers include active balance transfer checks which may be tied directly to a credit card account. These are often sent unsolicited, and may occur as often as once per month by some financial institutions. In cases where checks are stolen from a victim's mailbox they can be used at point of sales locations thereby leaving the victim responsible for the losses.

Countermeasures of card fraud

Over the past 25 years there has been a constant race between the credit card industry developing new security features to deter counterfeiting, and criminals working hard to compromise the technology and manufacture counterfeit cards. For safeguarding customers data, major card schemes including Visa, MasterCard, American Express, Discover, and JCB altogether constitutes Payment Card Industry Security Standards Council (PCI SSC). This council mandated an industry level security framework/global standard, PCI DSS (Payment Card Industry Data Security Standard) which has the most efficient and effective controls/ requirements to beat up various fraudulent activities of cyber-criminal by safeguarding card data.

Card fraud in Bangladesh

Recently some banks of Bangladesh are affected by card fraud. Investigation proved that, these fraudulent activities were done through skimming several ATM's. Central Bank has already mandated PCI DSS Compliance for branded (VISA, Master, JCB, American Express and Discovery) as well as non-branded (custom card by issuer) card through its ICT Guideline Version 3.0 Published May 2015.

Conclusion

Credit card fraud has been committed since credit cards were first introduced; however, modern technology has increased the ways in which it can be committed. Criminals see the card industry as a lucrative business that can be exploited by the use of technology. To counter the problem, credit card companies must constantly review security features and measures that are applied to card system. It's the right time for securing cardholder data by adopting PCI DSS through a PCI DSS Service Provider.

Source: all contributor in the www, PCI SSC, Right Time Limited (Bangladesh Based First and only PCI QSA Company)