CRC Bulletin

A Publication of CRC Credit Bureau Limited
www.crccreditbureau.com
Release No. 5; 1st July, 2013.

CRC Credit Bureau Limited
In association with Dun & Bradstreet

Identity Theft & Some Common Means Used by Criminals

Identity Theft occurs when someone obtains and uses information that personally identifies you, for example, your name, identity or credit card information, without your permission, in order to commit fraudulent transactions.

Some Common Ways Used By Criminals

- **Phishing.** This is the most common identity theft scheme. Identity fraudsters can pretend to be financial institutions and send spam or pop-up messages in order to get people to reveal their personal or credit card information.
- **Skimming.** Debit or credit card numbers can be obtained through the use of storage device when processing is being made on the card.
- **Man-in-the-Middle Attack.** This type of theft involves criminally intercepting communication between two parties and recording the information without the two parties ever knowing about it. The criminal then uses this information to access accounts and possibly steal the user's identity.
- **Shoulder Surfing.** This may occur anytime you use a password or a device that stores PIN numbers, such as at an ATM. The identity thief may attempt to get close enough to record the password or PIN numbers.

Protection Tips to Prevent Identity Theft

- Making the habit of periodically checking your credit reports, from a Credit Bureau helps you discover if anyone made unauthorized purchases or has stolen your identity to access your bank accounts or open other lines of credit in your name. CRC Credit Bureau offers customers a Self Enquiry report in order to assess submissions made by lending institutions with regards to your credit history.(Visit: www.crccreditbureau.com/self_enquiry/enquiry.html).
- Be aware of your surroundings when you are accessing any accounts that require you to enter a password or PIN in public. If someone stands too close to you, do not be afraid to ask the person to move back. If he/she is not willing to do so, let the person go first. Remember, it is better to be safe than sorry. If you do not feel safe, try using another machine.
- Do not write down your passwords where someone can find them, such as your wallet or purse. Also, take advantage of credit reports, which will help you analyze whether anyone has stolen your identity to access your bank accounts.
- Always check for the padlock symbol in the right-hand bottom of the website scroll bar if it is a merchant website. If it is an organization or an affiliation, contact the website administrator or the organization via phone or email to verify that such information is actually needed before entering in any information.