Tip of the Month – July 2010

Learning About Identity Theft -2
(It's Vacation Time Again)

"Don't worry, be happy" is the theme of a popular Caribbean song and you may just let your guard down while on vacation. However, the criminal never rests and is waiting to steal your identity if you relax a little too much.

Identity theft is the act of using someone's personal information - such as account number, driver's license. passport, national insurance number - and using the assumed identity to commit fraud or theft. Before you travel you can help reduce the risk that a thief will ruin your vacation by taking a few minutes planning before you leave home. You can also help avoid unnecessary problems with your financial institution. Here are some tips to assure an enjoyable vacation:-

- Ask your financial institution if they have a facility to identity "suspicious" transactions. Tell where you're going and indicate likely expenditure. Out of character charges may prompt a call to verify the transaction.

- Only carry two (2), credit cards (not the 3 or 4 many people have) and keep one of them apart from your wallet in case your wallet is lost or stolen.

- Leave your debit cards at home, these provide direct access to your accounts and are locally domiciled. You don't have these accounts emptied while you're away!

- If you use an ATM abroad, use one that always requires a personal identification number (PIN). It's also best to use ATM machines found at banks or credit unions that are in well-lit areas.

- Be sure to examine the ATM machine carefully for signs of tampering. Be on the lookout for anything that looks suspicious. Know how to identify skimming devices on an ATM or point of sale terminal.

- When dining in a restaurant, try to keep an eye on your credit card when you pay the bill.

- Leave your checkbook in a secure place at home. Use credit cards or traveler's checks instead.

- Leave your laptop at home, remember you are on vacation!

- If you must bring your laptop with you, be careful when using Wi-Fi networks. Most Wi-Fi hotspots are unsecured and unencrypted.

- If you are using cyber-cafés, hotel business centers, or other public access Internet facilities, be aware that keyloggers (software that can track your keystrokes) may be tracking you. Public access facilities may use servers that aren't encrypted. Therefore, never access any sensitive information from a public computer.

- Always be cautious with the information you share on social networking sites, such as FaceBook and Twitter. When you broadcast your travel plans on a social networking site, this information can then be used by criminals who will know that you will be away from home.

- Conduct a thorough clean-up of your wallet. Remove any unnecessary credit cards, your National Insurance card, and other unneeded documents that could compromise your identity if they were lost or stolen while on vacation.

- Photocopy or make a list of the remaining contents of your wallet. Keep it in a secure and locked location or with a trusted individual at home whom you can contact in case your wallet is lost or stolen.

- Do not leave your wallet or any documents containing personal information in your hotel room unattended. Hotel rooms are not the most secure places. Many people have access to the room. Use a hotel safe when available.

Taking these few precautions before you travel can help you avoid an unpleasant incident that could ruin your vacation.

Feel free to email us at dataprotection@bahamas.gov.bs