Consumer Council of Fiji
www.consumersfiji.org
CONSUMER COUNCIL OF FIJI

HEAD OFFICE
4 Carnavon Street
Private Mail Bag
GPO, Suva
Phone - General Office: 3300792, 3310183
Chief Executive Officer: 3305864
Fax: 3300115 | Email: **complaints@consumersfiji.org**

LAUTOKA/West
Suite 4 Popular Building
Vidilo Street
PO Box 5396, Lautoka
Phone: 6664987 | Fax: 6652846
Email: **consumerltk@connect.com.fj**

LABASA/North
Level 1, Lot 41 Raza Properties Ltd
Nasekula Road
PO Box 64, Labasa
Phone: 8812559 | Fax: 8812559
Email: **colbs@connect.com.fj**

19 April 2014 **Feature Article**

Identity Theft or ID Fraud

We all value safety and security when it comes to our money, our property and our name. A situation where some imposter steals your bank account details, your property details and your very name to siphon your money may be unimaginable, but is a very serious one that can result in huge personal losses. This is not a story anymore but a reality which is known as "Identity theft or ID theft".

Identity theft occurs when someone steals or gains unauthorized access to your personal information, such as your name, credit card number, or your passport details and uses these pretending to be you to commit crime or fraud or sometimes just to be mean.

The loss of personal information can hurt consumers. For example ID thieves can take your identity to create new debit/credit card accounts and change your billing address to a different address so that their activity is not detected. They use your details to make electronic withdrawals, until your account runs dry. ID thieves can also use your ID to obtain forged passport to migrate or use stolen details to get drivers license as a form of ID or file for fraudulent tax return pretending to be you to get a tax refund.

Sometimes they can also enter your online social network account to damage your reputation by posting malicious comments or embarrassing photos. Most reputable social networks have reporting and security mechanisms in place to prevent or detect such intrusions. For example, Facebook has a "Report a Problem" option.

Some of you may have received e-mails from someone purporting to be a friend or relative who is stranded in another country because the bag containing their passport and money was stolen or your friend or relative met with an accident and he/she needs money for emergency medical treatment. In such cases ID thieves collect the money.

A worst case of identity theft is when your identity is stolen by a thief who smartly secures your personal educational and professional details simply so he can apply for jobs, rent properties and obtain utility services.

There is a need for consumers to protect their identity in everyday activities and the best way is to fight identity theft is to **prevent** it in the first place. Here are some tips to prevent and protect your identity being stolen:

Regarding telephone scams:

- Do not give out your bank account number or other personal information over the phone. Hang up and dial the number of your bank to find out what the problem is. If the caller wants you to keep the call a secret then you should know it's a scam.
- If the caller claims you owe money or that there is a problem with your bank account, ask
- Beware and disregard text messages asking you to give money or notifying you that you have won some money.

Regarding the Internet:

- Every device that you use to connect to the internet should have up-to-date software including security software, operating systems, programs and other applications.
- Never send important personal information via email.
- Banks and financial institutions do not send email via web address like Yahoo! Gmail, Hotmail etc.

Regarding Wi-Fi Hotspots:

- Don't share personal information over an unsecured network (a connection that does not require a password for access). Using the direct web access on your phone is safer than an unsecured wireless network on your mobile device.

Limit your social networking

- Do not include basic information such as your full name and your date of birth in your online profiles. It is better to use a username rather than your real name.

Be wary of online shopping

- Make sure the site is legitimate. This includes a padlock on your web browser's address bar or a URL address that begins with http or https. These indicate that the purchase is encrypted or secured. For new sites, check online reviews.
- Save records of your online transactions, including the product description, price, online receipt, terms of the sale, and copies of email exchanges with the seller. Read your credit card statements as soon as you receive them to make sure there aren't any unauthorized changes.
- Check is the online trader has listed its physical address (e.g. street address), postal box number, phone and fax numbers which can be checked and verified.

If you suspect or uncover fraud, contact your bank, or the relevant organization. If its tax fraud contacts FRCA, if its drivers licence or permit, contact LTA if its passport ID theft contact Department of Immigration.