



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

26February 2014

Features Article

Banking Fraud

Can you imagine the shock you have to go through if you find out that your hard earned money has disappeared from your bank account through a mysterious transaction – this may sound bizarre to you but it is a reality and no longer just a crime story we read about or watched on TV. One Mr Singh of Suva faced his worst nightmare, falling victim to a bank fraud.

This is what Mr Singh had to go through as a bank customer:

Mr Singh who is illiterate relied on his friend, John, a tertiary student, to help him deposit and withdraw money from his bank account. John had access to all of Singh's personal details including his bank account number and even his bank balance. John also had a long-time friend working at the same bank where Singh had opened his savings account. John's friend being a banker had advised John that it was possible to register Singh for internet banking over the phone. He informed John of the procedures involved and what type of personal security questions would be asked in order to register. This allowed John to gather all the relevant information from Mr Singh. John finally called the bank to register Singh for e-banking and was able to get through the registration process successfully.

Mr Singh did not know he was being registered for e-banking. John then logged into Singh's account with Singh's username and password. He then registered himself as a payee and transferred \$12,000 of Singh's money into his (John's) account. John then proceeded to spend all this money as if it were his.

Mr Singh later on went to the bank to withdraw money. He learnt that his money was transferred into another account via online banking. Mr Singh was confused as he did not understand how an online account was opened for him when he always operated through his passbook.

He lodged a complaint with the Consumer Council of Fiji. The Council sought clarification from the bank concerned. Bank reimbursed \$12,000 to Mr Singh and the bank staff was terminated as a result of their internal investigations. Police was also notified.

This story highlights increasing concern over the way financial institutions verify just who is moving money around their systems.

So for now, as some consumers are finding out the hard way, only a username and password stands between criminals and their hard-earned money.

It is very important to understand that the security measures employed by most of the banks *can never be completely safe and secure*. To avoid such circumstance, consumers need to be **vigilant** with whom they share their personal information with.

Consumer responsibility:

While, banks must keep upgrading their security features to prevent such fraud, the burden lies heavily on the consumers to act responsibility to avoid such situations.

At no point in time, one must divulge his/her bank account details to anyone not privy to such personal information. Consumers must keep all their bank account details such as passbook, emails, username, passwords, PIN numbers, cheque leaf and correspondences with his/her bank in a safe place for these are private information, not to be shared.

Those consumers who are tech-savvy can use the Internet to regularly monitor online banking accounts for signs of fraud. The quicker a fraud is discovered, the easier it is to fix it.

Security tips:

- Do not give your bank detail to anybody or share your personal details as Mr Singh did. Keep your personal details along with all your financial details private;
- Do not write your PIN number on the access card or on your pass book or store these numbers in the wallet or handbag. Consumers doing this are at a greater risk.
- Check your account regularly. Report to your bank, especially if you think your card has been stolen, a suspicious transaction is on your bank statement, or your mail has been accessed by someone; and
- Choose password or PIN number which cannot be cracked.

Next week, read on e-banking