MOBILE MONEY, LOAN, ATM FRAUD & CRIME

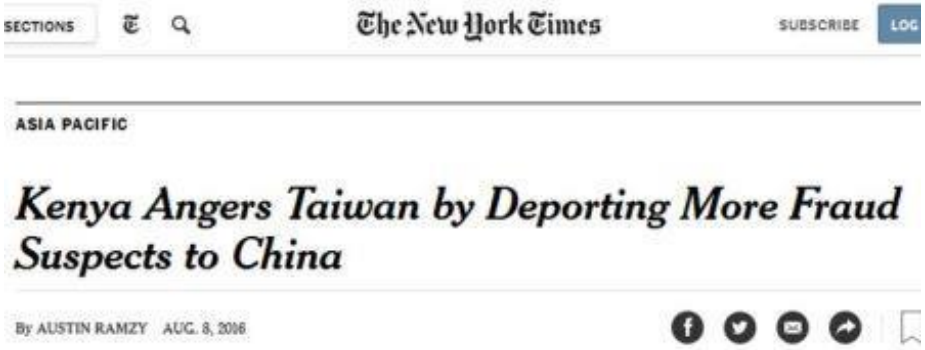
ICPAK

Annual Forensic Audit Conference

Dennis Muchiri
dennmuch@gmail.com

Thursday, 11th August, 2016

Heard of fraud lately?


SECTIONS

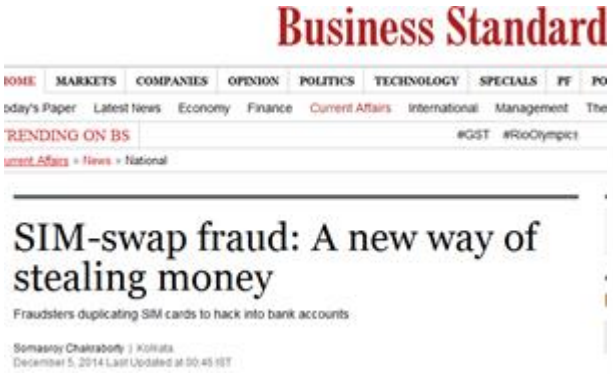
The New York Times

SUBSCRIBE LOG

ASIA PACIFIC

Kenya Angers Taiwan by Deporting More Fraud Suspects to China

By AUSTIN RAMZY AUG. 8, 2016


Business Standard

HOME MARKETS COMPANIES OPINION POLITICS TECHNOLOGY SPECIALS PF PO

Today's Paper Latest News Economy Finance Current Affairs International Management The

TRENDING ON BS #GST #RioOlympics

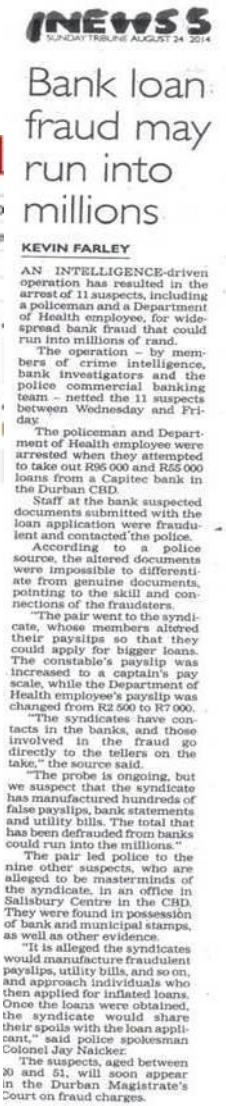
Current Affairs » News » National

SIM-swap fraud: A new way of stealing money

Fraudsters duplicating SIM cards to hack into bank accounts

Somasroy Chakraborty | Kolkata

December 5, 2014 Last Updated at 00:45 IST


INEWS

SUNDAY TRIBUNE AUGUST 24 2014

Bank loan fraud may run into millions

KEVIN FARLEY

AN INTELLIGENCE-driven operation has resulted in the arrest of 11 suspects, including a policeman and a Department of Health employee, for widespread bank fraud that could run into millions of rand.

The operation – by members of crime intelligence, bank investigators and the police commercial banking team – netted the 11 suspects between Wednesday and Friday.

The policeman and Department of Health employee were arrested when they attempted to take out R95 000 and R55 000 loans from a Capitec bank in the Durban CBD.

Staff at the bank suspected documents submitted with the loan application were fraudulent and contacted the police.

According to a police source, the altered documents were impossible to differentiate from genuine documents, pointing to the skill and connections of the fraudsters.

"The pair went to the syndicate, whose members altered their payslips so that they could apply for bigger loans. The constable's payslip was increased to a captain's pay scale, while the Department of Health employee's payslip was changed from R2 500 to R7 000.

"The syndicates have contacts in the banks, and those involved in the fraud go directly to the tellers on the take," the source said.

"The probe is ongoing, but we suspect that the syndicate has manufactured hundreds of false payslips, bank statements and utility bills. The total that has been defrauded from banks could run into the millions."

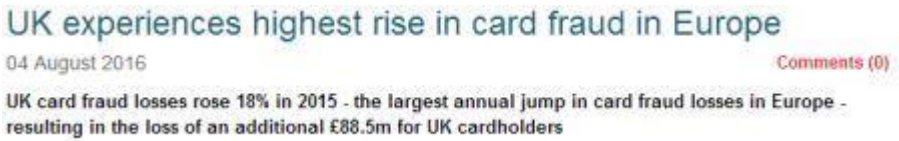
The pair led police to the nine other suspects, who are alleged to be masterminds of the syndicate, in an office in Salisbury Centre in the CBD. They were found in possession of bank and municipal stamps, as well as other evidence.

"It is alleged the syndicates would manufacture fraudulent payslips, utility bills, and so on, and approach individuals who then applied for inflated loans. Once the loans were obtained, the syndicate would share their spoils with the loan applicant," said police spokesman Colonel Jay Naicker.

The suspects, aged between 30 and 51, will soon appear in the Durban Magistrate's Court on fraud charges.

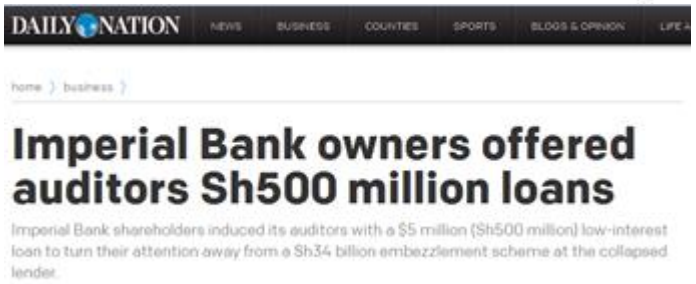
CRIME | Seven of the 11 Nigerians linked to the crime operate from Nairobi

FBI seeks Kenya's help to arrest bank fraud suspects


UK experiences highest rise in card fraud in Europe

04 August 2016 Comments (0)

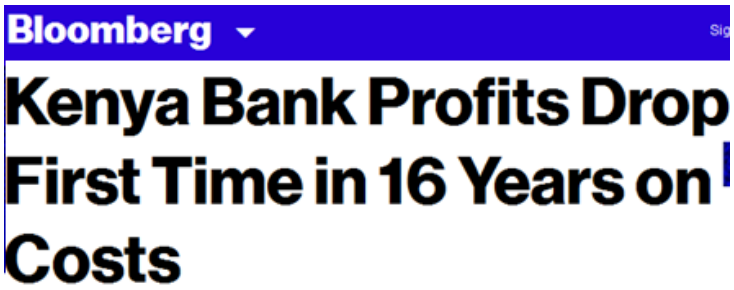
UK card fraud losses rose 18% in 2015 - the largest annual jump in card fraud losses in Europe - resulting in the loss of an additional £88.5m for UK cardholders


DAILY NATION NEWS BUSINESS COUNTIES SPORTS BLOGS & OPINION LIFE

home › business ›

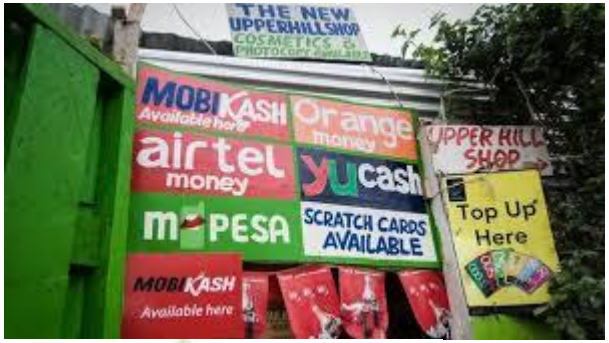
Imperial Bank owners offered auditors Sh500 million loans

Imperial Bank shareholders induced its auditors with a $5 million (Sh500 million) low-interest loan to turn their attention away from a Sh34 billion embezzlement scheme at the collapsed lender


Bloomberg

Kenya Bank Profits Drop First Time in 16 Years on Costs

Mobile Money (intro')



M-PESA

airtel money

Orange Money

MTN Mobile Money

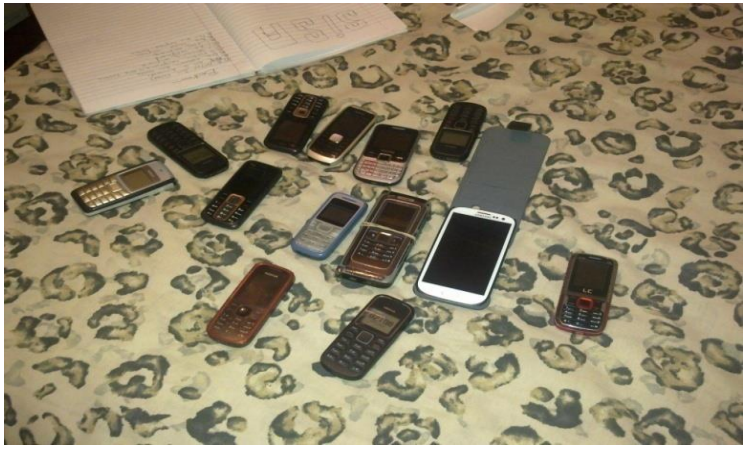
Equitel

- Financial services on mobile phone - deposit, withdraw, transfer money, pay for goods and services, m-banking, fundraise …
- >3bn mobile phones against <1bn banking accounts in the World - Frost & Sullivan
- Mobile Money products as having a 'greater impact than the Internet' on the lives of users - UK's Financial Services Authority
- M-Pesa, launched in 2007, has been the leading serving offering which has transformed Kenyan economy and lives. The service has over 20 million registered customers
- 43% of Kenya's GDP flowed through M-Pesa, with over 237 million person-to-person transactions (2013)

Mobile money – fraud

- Telecom industry estimates fraud losses due to mobile wallet fraud to be around 2-3% of mobile money revenues
- Fraud types
  - Phishing/Vishing/Smishing – personal information obtained usually through social engineering
  - Illegal SIM Swaps – use of fake identity documents or collusion
  - Identity theft
  - Advance Fee scams – duping of subscribers to send money
  - False transactions
  - Cyber attacks – intrusion of mobile money system and interfaces
  - Denial of service attacks
  - Agent malpractices – split transactions, remote withdrawals

SIM Swaps



- A rising number of frauds are perpetrated using mobile number takeover/hijack
- Personal information such as PIN, ID, DoB are compromised through;
  - Social engineering
  - Impersonation of telecom call centres/employees
  - Collusions
- Mobile banking fraud on the rise due to SIM Swaps

Loan Fraud

- An attempt to obtain funds which would otherwise be declined or to obtain funds on improved terms

- Loan Fraud Types
  - Forgery of documentation – The process of making and adapting documents with the intent to deceive or make money
  - Application fraud – Application fraud is when an individual or business knowingly submits incorrect or misleading information to support their application. Some examples include:
    i. Misrepresentation of financial information
    ii. Failure to disclose adverse bureau information
    iii. Use of a nominee to ‘front’ an application
    iv. Non arms length transactions / conflict of interest

Loan Fraud – a lending problem

- Many financial institutions do not recognize/report corporate lending fraud; it is often ‘hidden’ in impairment

- Experience shows that between 5-10% of impairment is due to fraud - higher in products like invoice financing and vehicle asset financing, and in sectors like the SME market.

- Many of the issues seen in retail lending business, such as collusion, are seen in the corporate lending too; but the size is bigger.

- Tough economic climate may force some honest customers into fraud to try to keep their businesses afloat as working capital dries up.

Loan Fraud – Red flags

- What are some of the indicators of loan fraud?

  - Contain spelling mistakes/mathematical errors
  - Font changes within the accounts
  - Irregular in format
  - Pages missing
  - Not Signed/dated
  - Dated immediately after the year-end
  - Records without accountant's name and address
  - No internet presence for the accountancy firm and contact details are a mobile number/yahoo email

ATM Fraud & Crime

- Card Jamming - ATM machine card reader is deliberately tampered with so that a client's card will be held in the card reader

- Card Swapping - client's ATM card is swapped for another card while undertaking an ATM transaction, without their knowledge

- Mugging - a client is physically attacked whilst in the process of conducting a transaction at an ATM machine, or just after completing a transaction at an ATM machine

- Skimming ("duplication") - copying data from the magnetic strips of credit and debit cards by swiping the cards through a reading device and then transferring the data to blank plastic cards, which are later used to make purchases at the victim's expense.

ATM Skimming

- Criminals tend to attach skimming devices either late at night or early in the morning, and during periods of low traffic.
- Skimming devices are usually attached for a few hours only.
- Criminals install equipment on at least 2 regions of an ATM to steal both the ATM card number and the PIN.
- Criminals then sit nearby receiving the information transmitted wirelessly via the devices (installed on the ATM).

Common Modus Operandi

Infiltration/Recruitment

- Infiltration of financial institutions
  - Which departments?
    - Operations, IT Department, Branches …
  - What is the new trend? eCrime
  - How do fraudsters identify their targets for recruitment?
    - Individual with insider knowledge - former bank staff members
    - Tribal connections: In some banks very predominant
    - Staff members with financial problems through the loan sharks with whom the fraudsters are connected
- Infiltration of Mobile Telco's. Why? SIM-Swap, Diversion of call-backs

Mobile money fraud – mitigation

- Awareness campaigns – customers and agents
- System Controls
  - Control access rights
  - User access and activity monitoring
  - Data protection
  - Penetration testing
- Transaction monitoring – data analytics
- M-banking – SMS alerts
- Mobile money accounts reconciliation
- Segregation of duties
- KYC controls
- Enabling regulation – AML etc.
- Effective training of employees

Lending fraud – prevention & detection

- Robust due diligence including Google keyword searches e.g. (Name), (Name + fraud), (Name + town)
- Meaningful conversations around track record
- Review the supporting documents and report any inconsistencies
- Validate the trading accounts where possible by cross referencing with Bank statements and VAT returns
- Don’t take things at face value, challenge where appropriate
- Exercise caution in relation to off-market transactions
- Report any suspicions or concerns to relevant department(s)

Tips to protect yourself

- Never ever let a waiter walk away with your debit/credit card
- Never give your PIN to family members (nor write it down)
- Hide with your hand the PIN you type on keyboard ATM
- Never accept assistance at ATM's
- Put your cheque book safely away
- Never reply to emails asking you to confirm your details
- Make sure that your PC has the latest anti-virus software
- When your mobile phone is suddenly no longer working go immediately to your telecom service provider and check your bank transactions
- Check regularly your bank statement
- When it sounds to good to be true, it is to good to be true.
  - You cant win a lottery in which you never participated
  - Unknown people who say they trust you and want to send you USD 20 million are fraudsters!

Protect your business

- Put your cheque book safely
- Understand that IT staff in your business are the new target by syndicates
- Finance payment platform:
  - Dedicated PC in secure area
  - Check regularly if no strange devices have been attached to your PC
  - Never reply to emails asking you to confirm your banking details
  - Make sure that your PC has the latest anti-virus software
  - Log-off PC when you leave your office
  - Use smart passwords
- Be aware of change banking detail scams (suppliers)
- When it sounds to good to be true, it is to good to be true.

… thank you.

Q&A