



The greatest ATM heist in history

By
Ramki



Truth many a time is stranger than fiction

- And hence Truth gets made into many a movie...
- 'Catch me if you can' was inspired by the greatest fraudster of all times Frank Abagnale Jr –who later became a FBI consultant!
- 'Special 26' from Bollywood was based on actual duping of a Mumbai jeweler TBJ by a guy masquerading as CBI officer with a bus load of recruits
- 'Goodfellas' was inspired by the 1978 Lufthansa Robbery
- I am sure the unbelievable Tobechi Onhuwara , Kenyan fraudster who was America's most wanted (he was recently caught after a 5 year hunt in Australia) and this \$45M heist have all the ingredients to be made into gripping movies!
- Let us look at this \$45M Cash-out scheme

The 8 perpetrators in NY

- One was the mastermind and the gang leader- Alberto Yusi Laijud –Pena
- Others were run of the mill people whom you would not have cast a second look
- Some were bus drivers, some, Kmart workers and one was a Pizza delivery boy
- Looted 3000 ATM's in 10 hours flat of a cool \$2.8M – the biggest in NY history
 - Cameras showed backpacks of a thief getting heavier and heavier!
- Suddenly these people starting spending like mad
 - Splurged on Rolex watches, new luxury cars and Miami trips
- Their sudden show off of their ill-gotten wealth led to their arrest!

The international gang

- Total \$45Million in 10 hours – an ‘Unlimited operation’
- The operation would put Interpol to shame!
- Associates in 26 countries with teams of cashers
- 4500 ATM withdrawals in 20 countries (RakBank) Nov 12- \$5M
- 36000 ATM withdrawals in 24 countries (Bank Muscat) Feb 13-\$40M
- Japan Operation most successful as some banks there allow upto \$10,000 per transaction in a single ATM
- Just 12 no limits compromised accounts of Bank Muscat did most of the damage!

The international gang

- Total \$45Million in 10 hours – an ‘Unlimited operation’
- The operation would put Interpol to shame!
- Associates in 26 countries with teams of cashers
- 4500 ATM withdrawals in 20 countries (RakBank) Nov 12- \$5M
- 36000 ATM withdrawals in 24 countries (Bank Muscat) Feb 13-\$40M
- Japan Operation most successful as some banks there allow upto \$10,000 per transaction in a single ATM
- Just 12 no limits compromised accounts of Bank Muscat did most of the damage!

Modus operandi

- Fraudsters hacked into the database of prepaid debit cards by penetrating Pune based Elctracard, Bangalore based EnStage and a unnamed US company which manage the transactions on prepaid cards
- Created counterfeit cards using data related to two mid east banks – RakBank of Ras-Al-Khaimah and Bank of Muscat of Oman –this can be done on even an expired credit card!
- Boosted the cash withdrawal limits
- Using ‘cashers’ emptied the accounts
- Laundered money thru purchase of luxury goods like Porche Panamera, Mercedes SUV, Rolex watches etc or just shipped money to global ring leaders
- Computer experts were watching all along the activity to ensure they got their due cut!

The world wide operation of US secret service

- Master card alerted US secret service
- They worked with Law enforcement in Japan, Canada, Germany, Romania, UAE, Dominican republic, Mexico, Italy, Spain, Belgium, France , UK, Latvia, Estonia, Thailand and Malaysia!
- Cracked most of the case , made arrests
- If convicted prison sentence could be 10 years
- Large chunk of loss will be borne by banks- RakBank has already provided \$4.7 M in its 2012 accounts

If you live by the sword , you die by the sword

- The leader Alberto escaped to Dominican republic
- He was hiding in his wife's cousin's place and they got suspicious
- Staged a drama to steal the money!
- Two hooded men entered the home where he was hiding and he drew his 0.45 caliber pistol- they shot him 5 times and fled
- Near by the body lay \$100,000 in an envelope which was not touched!

Why does this happen?

- Fraudsters target the weak links
- USA, Mid east (and India) still use old Magnetic stripe card technology –ditched by Europe -which is very easy to counterfeit
- USA target migration to new EMV technology is 2015!
- This coupled with ineffective transaction monitoring leads to fraud
- ATM fraud was around \$100M in 1980's
- By 2008 it was \$1B!
- This is easy, bloodless and can be done by anyone with internet connection and some intelligence!

Lessons

- What is required:
 - New technology –Chip and Pin
 - Strong PIN security
 - Real time and continuous transaction monitoring
 - Effective intrusion monitoring systems
 - Taking real care of insider threat
 - Good controls at outsourcing centers
 - More info sharing between law enforcement agencies
 - Collaboration among industry and banking institutions
 - Solid real time fraud solutions

Lessons for Indian outsourcing companies

- Key controls for detection of suspicious trading activity on real time basis not in place
 - Joint probe by British and Swiss regulators post UBS \$2.3B loss caused by a rogue trader
- Financial crime training in India needs better support from host countries like UK
 - Report on outsourcing by HDBC and Stanchart by Uk Financial market regulator FCA
- Fake CV's, inconsistent references and previous employer reluctance to provide references leads to ineffective checking of bonafides of Indian employees. Lack of electronic database infrastructure to allow fast and effective reference checking
 - US Federal deposit insurance reports and others
- If we want to continue to be world's back office , we need to address these asap.

Sources

- Why We Can Expect More ATM Cash-Outs - BankInfoSecurity
- ATM heist A splashy trail of big spending - The Times of India
- The great \$45m bank cyber-heist Seven New Yorkers cuffed • The Register
- Cyber cheats hacked Pune, Bangalore companies - The Times of India
- Global network of hackers steals \$45M from ATMs - WSJ.com
- Indian outsourcing under lens after \$45 million ATM heist - The Times of India
- In Hours, Thieves Took \$45 Million in A.T.M. Scheme - NYTimes.com