

AML/CTF in South Africa

'New technology and new risks?' and
the 'regulator's dilemma'

September 19th, 2007

EISENHOWER BANK

A division of Broadway National Bank. Member FDIC.

Toll-Free 1-888-777-0740



[HOME](#)



[REQUEST
MORE INFORMATION](#)



[SITE MAP](#)

[Online
Banking](#)

[Mobile
Banking](#)

[Checking](#)

[Savings](#)

[Loans](#)

[Worldwide
Banking](#)

[Current
Rates](#)

[ATM and
Debit Cards](#)

[Other
Services](#)

[E-mail
Registration](#)

[Useful Military,
Other Links](#)

[Locations](#)

[Pre-
Deployment
Checklist](#)

[History](#)

[Employment
Opportunities](#)



Please Note: Eisenhower Bank will never ask for your Social Security numbers, account numbers or passwords in any email. If you have received emails requesting this type of information, please delete immediately.

[Click here for more information](#)

Teba Bank Target Market: risk profile

- Existing market of lower income employees of the mining industry and their dependents
- Low income households in rural areas
- Communities living and working around mining towns

Accounts opened:

- Automatically on request of mine employer
- At branch or agent (Teba Ltd.)
- At government department (UIF) with EFT POS
- Real time transaction monitoring

AML in South Africa

- FIC Act 2001 establishing reporting obligations
- Staff training and testing
- Client registration requires identification and verification of:
 - Full name
 - Date of Birth
 - ID number (national ID)
 - Residential address
- “reasonably practical means” “if believed reasonably necessary”
- Financial Services Charter 2004 – greater access

Exemption 17, 2002 (2004)

- Maximum balance R25,000 (\$3,570)
- Maximum transaction value R 5,000 (\$714) (R25,000 per month)
- No international transactions (other than cash withdrawals in Common Monetary Area)
- One such account per person

MTN Banking

- Joint venture between Standard Bank and MTN – a mobile banking business
- Branded MTN
- Risk and compliance responsibility of Standard Bank (a division of Standard Bank)
- Registration process from own phone “self service” no requirement to visit a branch (Exemption 17 limitations)

FIC Act

- “No accountable institution may knowingly establish or maintain a business relationship or conduct a single transaction with a client who is entering into that business relationship or single transaction under a false name”
- Regulation 18 – Non face to face verification: banks must take “reasonable steps” to confirm the existence of the client and verify the identity of the natural person involved
- Core principles – that banks should apply equally effective customer identification procedures and ongoing monitoring standards for non face to face customers

Non face to face process

Launch August 2005 and misleading press coverage

Meetings with FIC August, September and November 2005 and February 2006 to discuss non face to face verification and risk mitigation

Perceived product risks

- Ability to easily open a large number of accounts and move the money buying pre paid SIMs and a list of ID numbers
- Ability to open a large number of accounts and move off shore
- Large number of accounts opened by different members of syndicate and SIM cards handed over for use by leader
- Criminals opens account and throws away phone and SIM card, only transacting using debit card and ATM – therefore less traceable
- Suspicious transactions
- Large amounts of cash deposited into account

Proposal for regulation

- Limitations on balance and transaction values as for Exemption 17 for face to face
- Daily transaction limits lower for non face to face - *Became R1,000 (\$145)*
- Geographical limits for transactions – within SA except for cash withdrawals within CMA
- One account per ID and per SIM card
- Natural persons who are SA citizens and permanent residents
- Minors supported by a guardian

Risk management on registration – 2006 Cell Phone Banking Regulation

- ID number checked for being a validly composed number
- Confirmation that no other account held for that ID number
- ID number checked against Dept of Home Affairs data base or other reliable third party data base for match with name, death records and emigration records
- Check ID number against Dept of Justice data base (or other reliable data base) for fraud convictions
- Check name given by client fully compliant with name returned by data base
- Daily or real time monitoring for suspicious transactions – velocity checking, pattern recognition etc. (became '*enhanced measures to scrutinise transaction activity to be able to identify and report suspicious and unusual transactions*)
- "*Continue to explore ways to enhance non face to face account opening to ensure that the information actually pertains to that person*"

Future developments

- Telco regulations: KYC requirements for pre paid SIM cards - opportunity
- Development of field registration system
- Training additional FICA agents (MTN)
- Using existing FICA agents e.g. insurance brokers
- Using other data bases
- Need for cheaper more efficient ways to implement customer verification (FIC Directors Report 2006)