



Fraud and Security Awareness

A Presentation by

The Inter-Bank Fraud Awareness Sub-Committee
Bankers' Association of Trinidad and Tobago



Fraud

“A Local Perspective”

Presented by Terrence A. M. Butcher





The Nature of Fraud

Fraud by nature, involves **betrayal** of **trust** or **deception**. The fraudster does not use force or violence, but instead manipulates or exploits the trust and respectability that they have built up in their relationships with people.....they prey on their victims' gullibility or greed.



FRAUD DEFINED.....

An intentional perversion of the truth, for the purpose of inducing another, in reliance upon it, to part with some valuable thing belonging to him/her or to surrender a legal right.

Black's Law Dictionary

e.g. a false story told to induce a victim to part with his money.



WHAT ARE THE MOTIVATORS?

“GONE”

G – Greed

O – Opportunity

N – Need

E – Expectation of being caught is low



PERCEIVED JUSTIFICATION

“I am just borrowing the funds”

“I am not hurting anyone, the company can afford it”

“I am underpaid so this is my bonus”

“Everyone else is doing it so why not me”

“The company’s funds are insured and would not lose”

“It is a challenge to me”

“I am sure this person has more money than me...”



FRAUD SCHEMES IN T&T

Internal frauds:

embezzlement, false accounting,
forgeries, payroll & billing schemes, etc.

External frauds:

forgeries, uttering, issuing dishonoured
cheques, fraudulent conversion,
computer frauds, theft of credit card
data.

FRAUD TYPOLOGIES

CREDIT
CARD
FRAUD



FRAUD TYPOLOGIES

Card Present

TYPE	DESCRIPTION	CONTROL MEASURES
LOST/STOLEN CREDIT CARDS	Cards are lost or stolen and subsequently used by unauthorized persons	Merchants – Verify signature on card and slip. Request ID if unsure. Cardholders – Do not leave cards unattended etc. Report loss immediately.

FRAUD TYPOLOGIES

Credit Card Skimming





FRAUD TYPOLOGIES

CARD SKIMMING (mainly credit cards)

Magnetic information is lifted or copied onto a small hand-held device called a skimmer. The information is downloaded to a computer and then onto a plastic card. This could be either a lost/stolen card, a counterfeit card, or a blank plastic card.

Merchants – observe employees and pay attention to any unusual behaviour.

Cardholders – Ensure that the card is never out of your eyesight.

FRAUD TYPOLOGIES

Card Not Present



**INTERNET
Phishing
E-Mail
Telephone Calls**

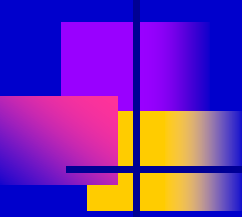
>Pop-up windows appears
“Congratulations! You Have Won...”

>Unsolicited E-mails requesting information about your account under the pretext of conducting a survey or from your bank or Card Associations such as Visa or MasterCard under the pretext of verifying transactions

Do not disclose any information on your account to anyone. If the Bank is calling you they already have your account number and expiry date. Report the incident immediately to your bankers.

FRAUD TYPOLOGIES

Card Not Present



INTERNET Phishing E-Mail Telephone Calls	Telephone calls received requesting card information for verification purposes.	Do not give out information over the telephone to anyone. The bank already has that information.
---	---	--

FRAUD TYPOLOGIES

Card Not Present

TYPE	DESCRIPTION	CONTROL MEASURES
INTERNET	Account information, including account number, expiry date, and CVV/CVC is stolen and used by unauthorized persons for ecommerce transactions.	Properly dispose old receipts, statements, letters etc.

Fraud Typologies

ATM
FRAUD





FRAUD TYPOLOGIES

ATM
MANIPULATION
LEBANESE LOOP
CARD SWAPPING
SHOULDER
SURFING

Cards trapped /
PIN
compromised
Unauthorized
withdrawals /
purchases

Cardholders –
Do not disclose
your PIN to
anyone. If the
card is stuck in
the ATM, report
it immediately to
your bankers.
Protect your
card and PIN
from view.



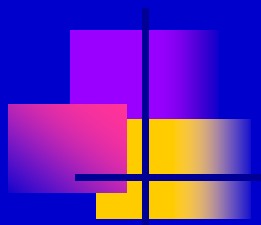
FRAUD TYPOLOGIES

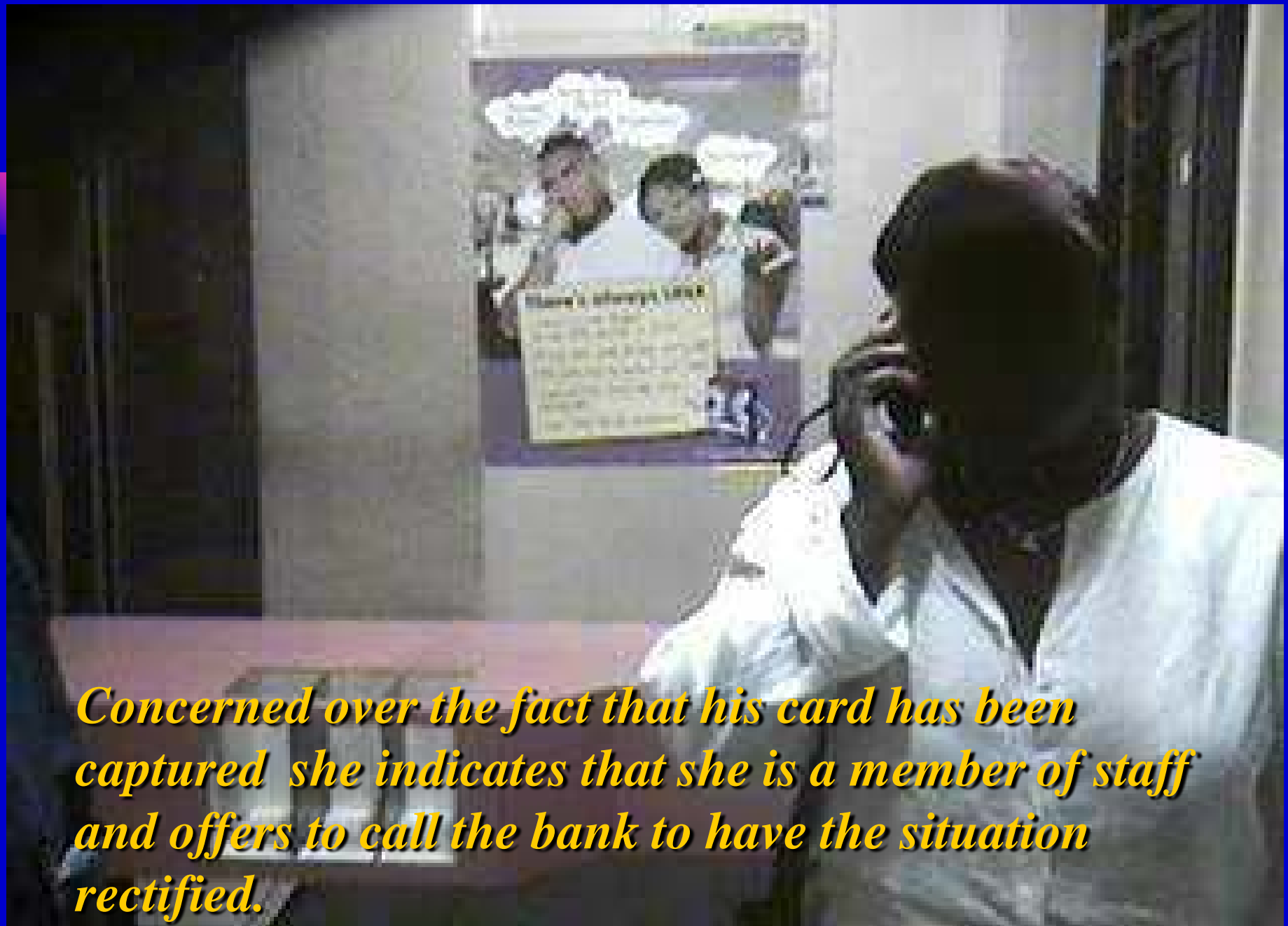
ATM TAMPERING
LEBANESE LOOP
CARD SWAPPING
SHOULDER
SURFING

Cards captured
in ATM and
assistance from
unauthorized
persons is
offered.

Cardholders –
Do not disclose
you PIN to
anyone. If the
card is stuck in
the ATM, report
it immediately.
Protect your
card and PIN
from view.

Shoulder Surfing





Concerned over the fact that his card has been captured she indicates that she is a member of staff and offers to call the bank to have the situation rectified.

The customer is even given the cell to talk to the bogus card centre representative.



He willingly accepts the cell phone and follows the instructions give to him by the individual on the other end.





The instructions call for the customer to disclose his PIN so that the card centre representative can reactivate the machine.



The customer discloses his PIN to the individual and follows the instructions however the card does not eject. He is then advised to collect it tomorrow morning.



FRAUD TYPOLOGIES

Credit Card Skimming





FRAUD TYPOLOGIES

CARD SKIMMING (mainly credit cards)

Magnetic information is lifted or copied onto a small hand-held device called a skimmer. The information is downloaded to a computer and then onto a plastic card. This could be either a lost/stolen card, a counterfeit card, or a blank plastic card.

Merchants – observe employees and pay attention to any unusual behaviour.

Cardholders – Ensure that the card is never out of your eyesight.



FRAUD TYPOLOGIES

CHEQUE FRAUD



FRAUD TYPOLOGIES

CHEQUE FRAUD

Counterfeit Cheques
Altered Cheques
Forged Cheques

Cheques are stolen, created, altered and/or signatures and endorsements forged to pass off to unsuspecting individuals, businesses or financial institutions as genuine.

Protect any unused cheques and statements.
Familiarize yourself with security features.
Contact the issuing bank when in doubt.
Ensure that you obtain valid ID.



FRAUD TYPOLOGIES

**IDENTITY
THEFT**



FRAUD TYPOLOGIES

IDENTITY THEFT SCHEMES

Person assumes the identity of another in order to perpetrate fraud in the assumed name. Common schemes involve encashing lost/stolen cheques, account takeover schemes, etc.

Always try to confirm ID, request another when in doubt. Protect account information, statements, insurance, tax and other sensitive documents. Shred unwanted documents that contain account information. Beware of persons who rummage through your trash.



TODAY'S CHALLENGES

New technology being adopted by fraudsters.

Computers, software, scanners, printers, skimming devices etc.

Ability to corrupt employees in organizations to facilitate fraud.

Level of expertise being recruited into fraud syndicates (including deportees with history in sophisticated frauds)



STRATEGIES

- New/Revised Legislation required to assist law enforcement efforts.
- Law Enforcement and Forensic Professionals would require on-going upgrade of skills and training to treat with the onslaught of new fraud technology and trends.
- Ongoing merchant/customer awareness training and education.
- Maintain inter-agency and inter-bank liaison, intelligence gathering and sharing.
- Assistance to Policing Agencies – equipment etc..



Security Awareness “Jungle Warfare”

Presented by Hayden De Four



Jungle Warfare

How can the prey defeat the predator?

Presented By: H. De Four

BATT Banking Week – Partnering with you for a New Economy

The Impala and the Lion





Side by Side Comparison

Impala

- Height – 1m
- Weight - 65kg
- Speed – 61mph

Main Advantage

- Distance covered
33ft
- Airborne 10ft

Lion

- Height – 1.22m
- Weight – 191kg
- Speed – 50mph

Main Advantage

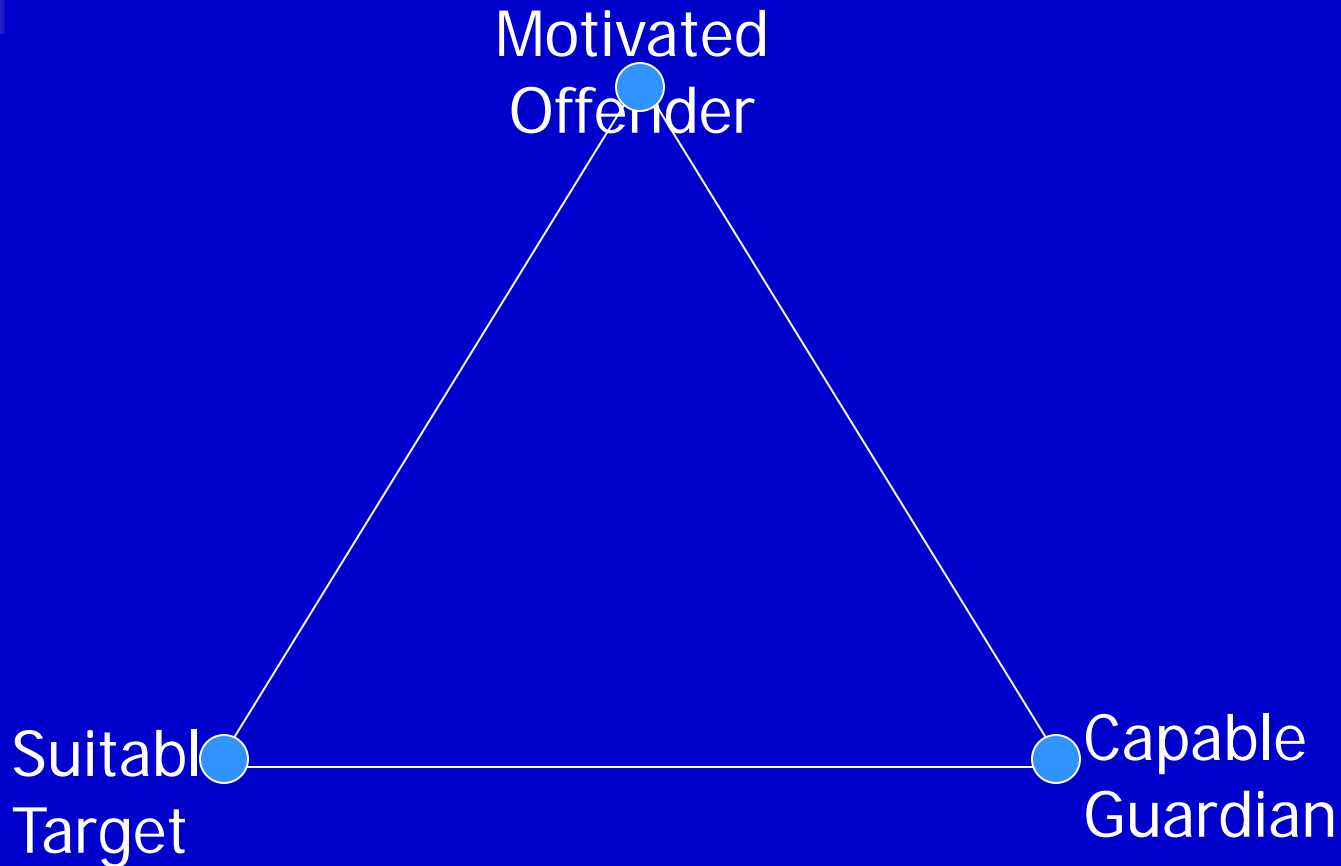
- Strength
- Operate in groups

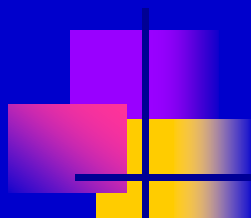


Feeling the paradigm shift?

- Which one has the winning advantage?
- Does the lion's characteristics remind you of anyone?
- How can the impala defeat the lion????

Where does the Impala fit in the Crime Triangle?





Predatory Crime, does the Impala
have a fighting chance?



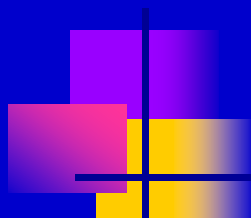
Cooper's Colours

- White – The Sleep or the dream state. Totally unaware of one's surroundings.
- Yellow – A state of relaxed alertness. You are aware of your surroundings and not yet aware of anything warranting closer attention.
- Orange – You are aware of a threat scenario and are focused on evaluating it's potential for danger.
- Red – Something has occurred and you are now at the fight or flight stage.
- Black – You are in a state of shock



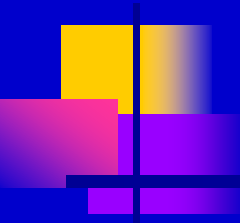
Your concerns?

- Rising Crime Levels increase the risk associated with doing business
- Reports of robbery of customers en route to and from the Bank
- Privacy concerns
- Involvement of Bank staff in Robberies



How can the impala defeat the
lion????

Scenario #1



Transacting at the Branch



The cunning Impala will...

- Seek to transfer that risk to a CIT Provider
- Where he/she is not so inclined, he/she must ensure that they operate in threat condition yellow
- Have a plan
- Practice proper journey management
- Know the fundamentals of surveillance (both vehicular and foot)



Scenario #2

Depositing via the Night Safe



The Cunning Impala will...

- Transfer the risk to a CIT provider
- Where he/she is not so inclined, he/she should assess the risks and devise a plan
- Operate in Threat condition Yellow but be ready to change to a higher level instantly
- Practice Journey Management
- Know the principles of surveillance



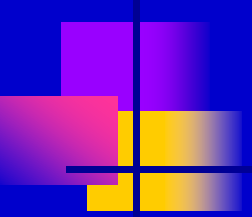
What have we learned?

Does the Impala have a fighting chance?



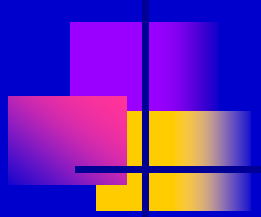
The Impala will thrive once...

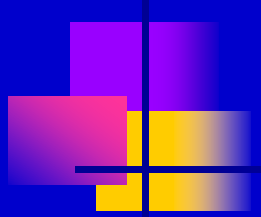
- He/she is aware of the environment within which he/she operates
- He/she prepares for the day by taking cognizance of the threats within the environment
- He/she utilizes his/her innate skills to ward off an attack



While the predator chooses the time, the location and method of attack, it is only you that will determine your response to the situation.

It is that level of uncertainty that affords you the chance to be victorious.





The End

Any Questions ?

Thank You.