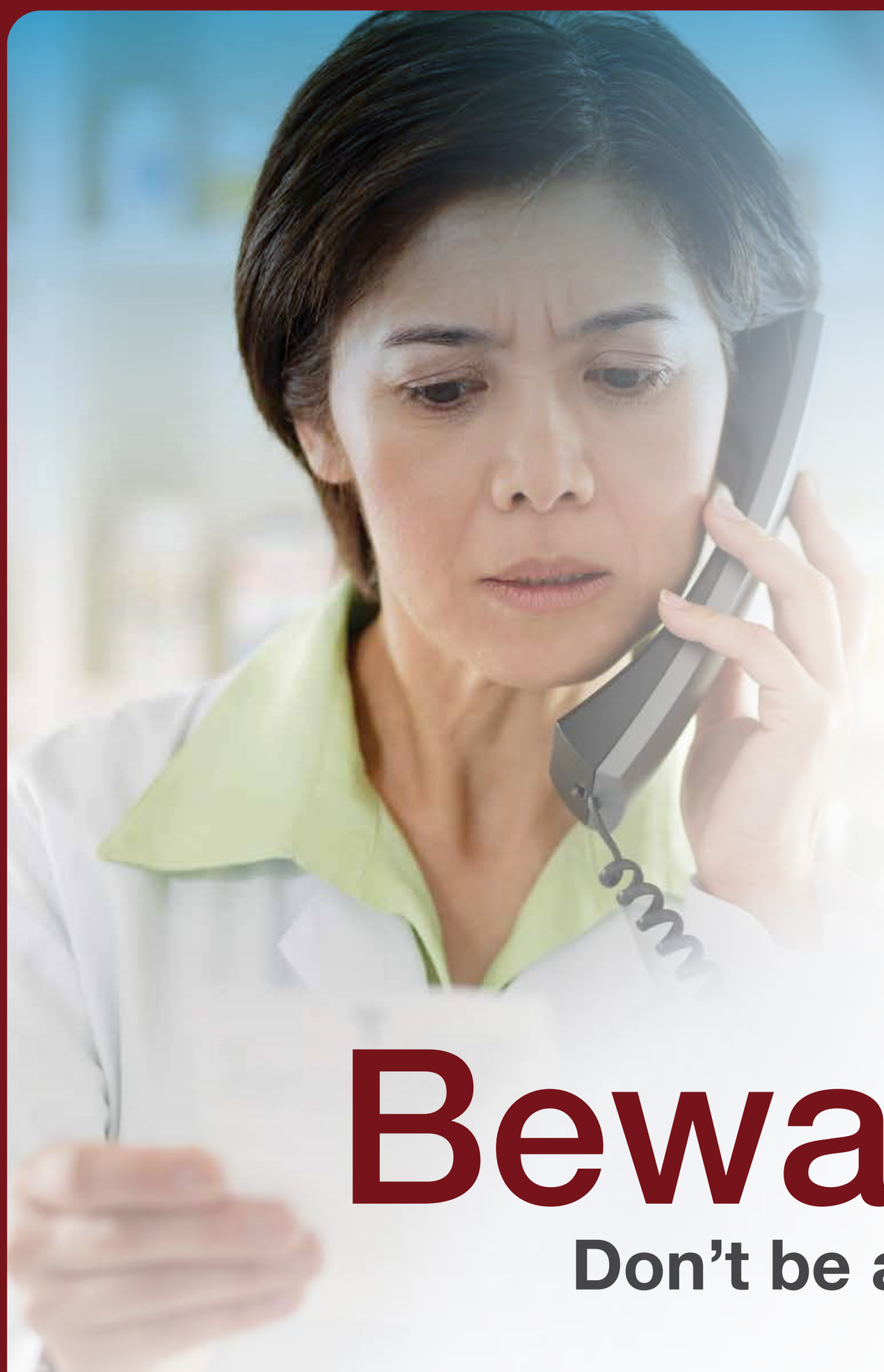

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Your credit card has been cloned...

Someone has stolen your identity...

Your account has been tampered...

Beware!

Don't be a SCAM victim.

CAUTION on BOGUS CALLS and MESSAGES claiming to be from Bank Negara Malaysia, private bank, utility provider or an enforcement agency.

It's a SCAM. Do not panic. Think straight.

1. Bank Negara Malaysia **never requests** for your personal or financial information
2. Bank Negara Malaysia **never asks** anyone to transfer money to any 3rd party account
3. Bank Negara Malaysia **never keeps** public's money in any account

When in doubt, please call

BNMTELELINK (Customer Service Call Centre)

1-300-88-5465

Fax: 03-2174 1515 Email: bnmtelelink@bnm.gov.my

To submit SMS enquiries or complaints, type : **BNM TANYA [your enquiry/ complaint]** and send to **15888**

For more information please refer to the **Financial Fraud Alert** available on Bank Negara Malaysia's website

www.bnm.gov.my

BNMLINK (Walk-in Customer Service Centre)
Bank Negara Malaysia Kuala Lumpur (Block D, Jalan Dato' Onn, 50480) or visit BNMLINK branches in Bank Negara Malaysia: Johor Bahru, Penang, Kuala Terengganu, Kota Kinabalu and Kuching
(Business hours are: Monday - Friday, 9:00 am - 5:00 pm)

Fraud Awareness

What is Fraud?

Fraud is the criminal intention to deceive, cheat or trick someone, whether a person or an entity to gain an advantage such as money, power, authority and materials.

Target Victims

Anyone can be a target victim. However, most victims are those who are gullible or greedy.

Identity theft

Identity theft can be divided into two broad categories: Application fraud and account takeover

Application fraud

Application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name without authorization. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. Alternatively, they may create counterfeit documents

Account takeover

Account takeover happens when a criminal tries to take over another person's account, first by gathering information about the intended victim, and then contacting their card issuer while impersonating the genuine cardholder, and asking for mail to be redirected to a new address. The criminal then reports the card lost and asks for a replacement to be sent.

ATM Skimming

Skimming is the theft of credit card information used in an otherwise legitimate transaction. The thief can procure a victim's credit card number using advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victims' credit/debit card numbers. The perpetrator has put over the card slot of an ATM (automated teller machine) a device that reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a miniature camera (inconspicuously attached to the ATM) to read the user's PIN at the same time. This method is being used very frequently in many parts of the world. Another technique used is a keypad overlay that matches up with the buttons of the legitimate keypad below it and presses them when operated, but records or wirelessly transmits the keylog of the PIN entered. The device or group of devices illicitly installed on an ATM are also colloquially known as a "skimmer". Recently-made ATMs now often run a picture of what the slot and keypad are supposed to look like as a background, so that consumers can identify foreign devices attached.

Phishing

Phone scam

The fraudster usually attempts to obtain sensitive information over a voice call. The fraudster normally tries to gain the victim's trust by impersonating a credible individual such as a banking authority or a police investigation officer. Victims may not verify the received calls purportedly made by such persons thinking that the calls are from regulators so called, to avoid embarrassment or as a result of "warnings" given by the "officer".

Email scam

An email scam is a type of scam more widely known as 'phishing'. An email scam involves a fraudster randomly sending forged emails purportedly from financial institutions or publicly known organisations to lure victims into revealing their internet banking login credentials, email credentials, credit card numbers, bank account numbers and/or passwords which are then used to perform transactions not authorised by the victims. These emails are designed to appear legitimate to gain the trust of the recipient. The content of the email typically attempts to inflict a sense of urgency and panic in order to trick customers into revealing confidential information on a fake website/popup.

SMS scam

A SMS scam usually involves SMS-es initiated by a fraudster to trick victims into believing that they have won a contest/reward and which attempt to lead them into compromising their banking information and/or create an internet banking facility without the victim even realising it.

This type of scam may also involve 'identity theft' since an unauthorised person usually pretends to be a valid account holder and accesses the customer's account (usually through the internet), unbeknown to the account holder.

Security tips

- As soon as you receive your new card, sign it.
- Treat your card like cash. Safeguard it at all times.
- Keep a vigilant eye on the card, wherever the card is, whether in your bag, pocket, drawer or at the cashier, especially when it is out of your sight.
- Ensure the card is not left unattended.
- Check that it is your own card (name and account number) that is returned to you after any transaction.
- Any card loss must be reported to the card issuer and police immediately.
- Check the amount on the sales draft before signing.
- Do not sign blank, incomplete or altered sales draft.
- Destroy any altered or mutilated sales draft before throwing them away.
- Do not lend your card to anyone.

Protecting Your ATM Cards

Do's

1. Keep your receipts and use them to check entries against bank statement/ passbook regularly.
2. Memorize your PIN, and then destroy the PIN notification.
3. Change your PIN periodically.
4. Keep your card clean.
5. Keep your card in a safe/secured place.
6. Report immediately to your bank if your ATM card is lost / stolen or your balance is incorrect

Dont's

1. Do not allow a third party to transact on your behalf.
2. Do not keep your PIN in the same place as your card.
3. Do not keep your PIN in your address book or diary.
4. Do not keep your PIN in an unlocked drawer.
5. Do not keep your PIN in your wallet or purse.
6. Do not leave your card in your briefcase, car or office drawer.
7. Do not use the ATM if you see unusual or suspicious apparatus attached to the machine.

How to Avoid being a Victim?

- Follow the simple rule of 'if it is too good to be true it normally is'.
- Do not perform transaction on websites opened via email links.
- Ensure your cheque book is kept safe. Do not pass your cheque book to anyone.
- Do not compromise your ATM PIN, UserID, Password, security documents (such as identity card, legal documents, etc) or other personal identification tags.
- Always ensure that all credit card transactions are performed in front of you. Do not let the card get out of sight.
- Inform Association of Banks in Malaysia (ABM) if you have lost your identity documents or believe your identity documents could have been compromised (after lodging a police report).
- Always deal directly with your banker or authorised agents. If not sure, check with your banker, authorised agents or relevant authorities.

Contact the following

- If it relates to Standard Chartered Bank Malaysia Berhad.
  Contact Standard Chartered Bank Malaysia Berhad Customer Care
  local 1 300 888 888 and overseas +603-7711 8888 or
  email: Malaysia.Feedback@sc.com.
- BNMTELELINK at 1 300 88 5465
- Your banker, if it relates to other banks.
- Association of Banks in Malaysia (ABM) at 1 300 88 9980.
- Polis Diraja Malaysia.