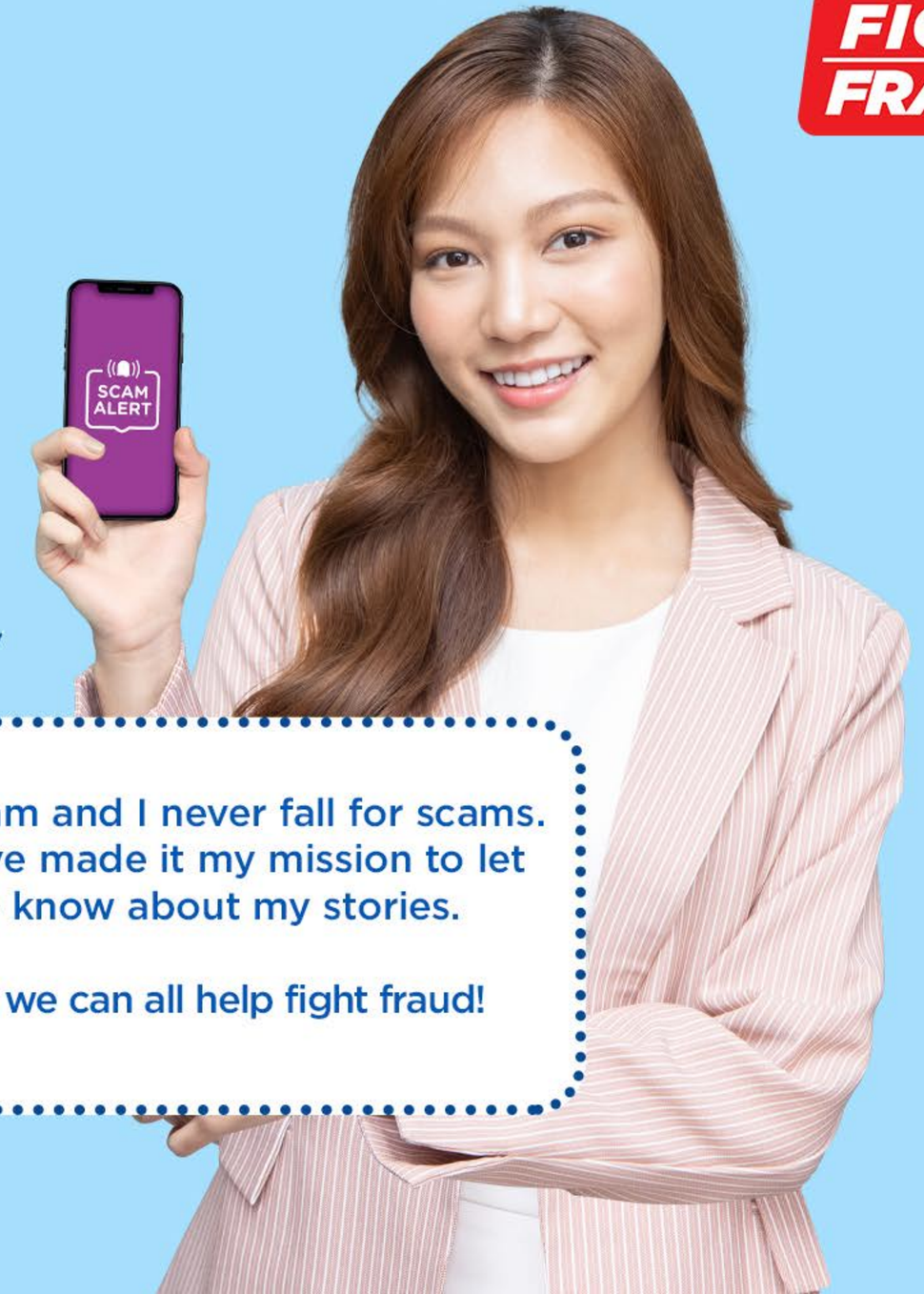
FIGHT FRAUD

SAM AGAINST SCAMS



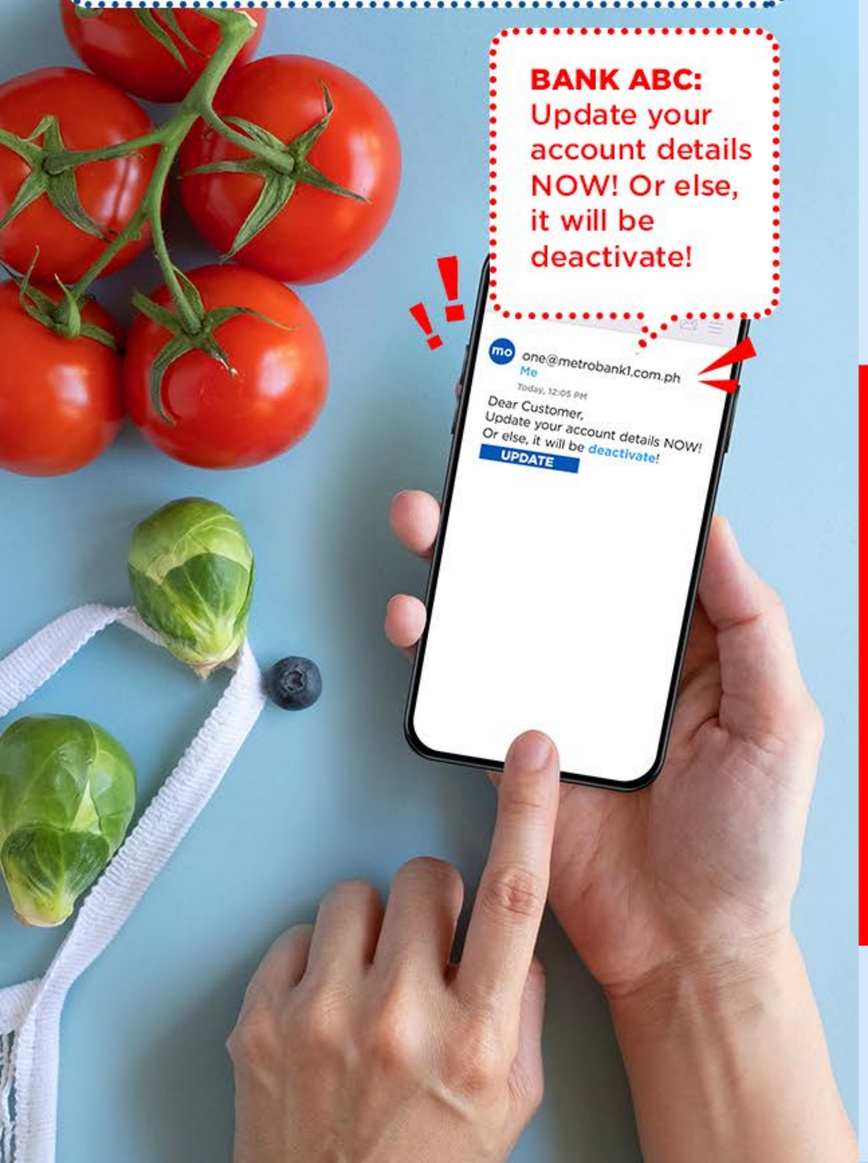
Hi, I'm Sam and I never fall for scams. Today, I've made it my mission to let everyone know about my stories.

Together, we can all help fight fraud!

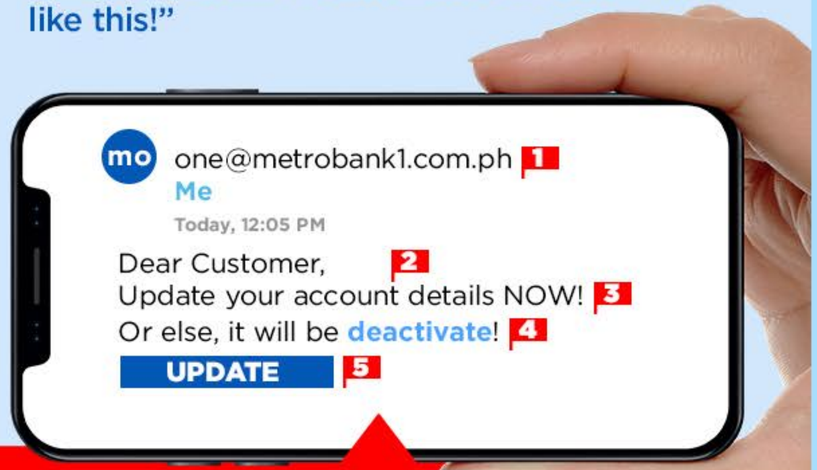
Metrobank
You're in good hands

TABLE OF CONTENTS

I was cooking our lunch one Saturday afternoon, when:



"My heart pounded fast. It was a Phishing email! My bank would never threaten me like this!"



RED FLAGS

1. **Wrong email address of bank**
2. **Asking for online banking username and password, as well as your OTP**
3. **Threatening statement and sense of urgency, so you will have no time to think**
4. **Wrong spelling or grammar**
5. **A suspicious link or button**

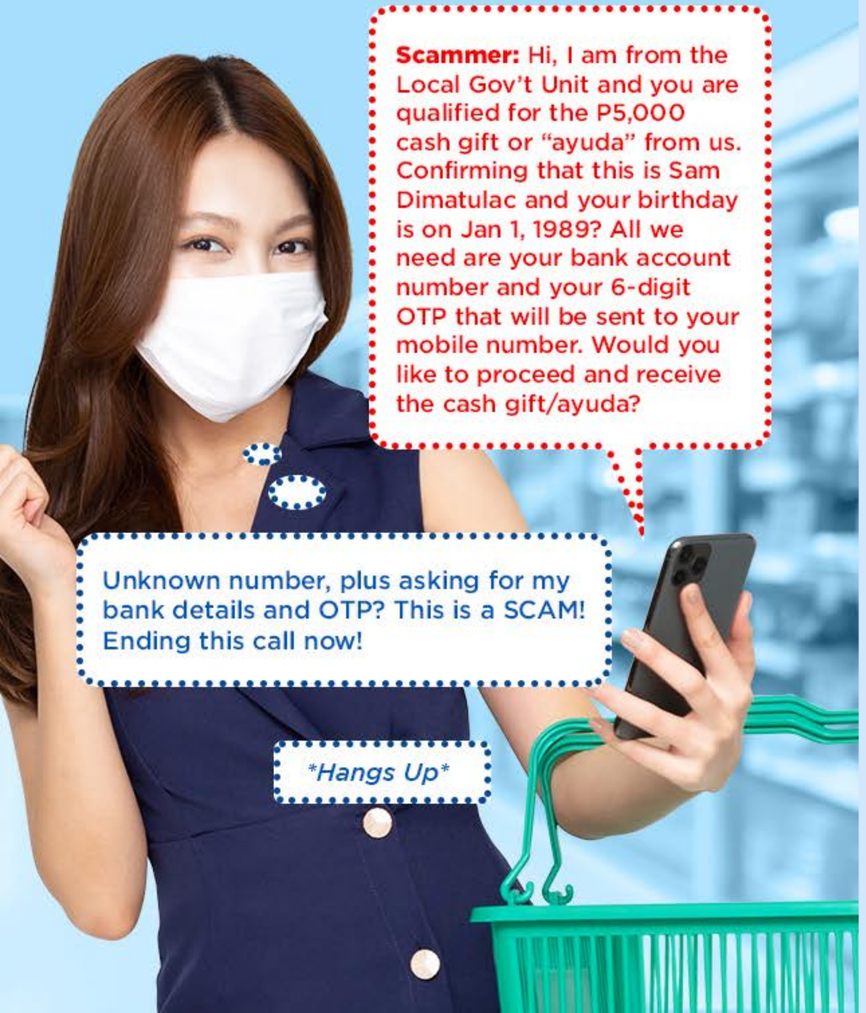
"I checked my account afterwards and it was intact. That's a scam-free day for Sam!"

ANTI-SCAM TIPS BY SAM

1. DO NOT REPLY or click on any unverified links or buttons.
2. Forward the said message to your bank. In my case I reported it to: **customercare@metrobank.com.ph** and used **REPORT ON POSSIBLE FRAUD** as the title of my email.
3. Never give your account and card details, as well as your OTP.
4. Manually type the official bank website address on your browser or use the Metrobank Mobile app.

SAM-1 vs SCAM-0

I was at the grocery store when I got a call from an unknown number.



"That was such a suspicious call with so many RED FLAGS!"

RED FLAGS

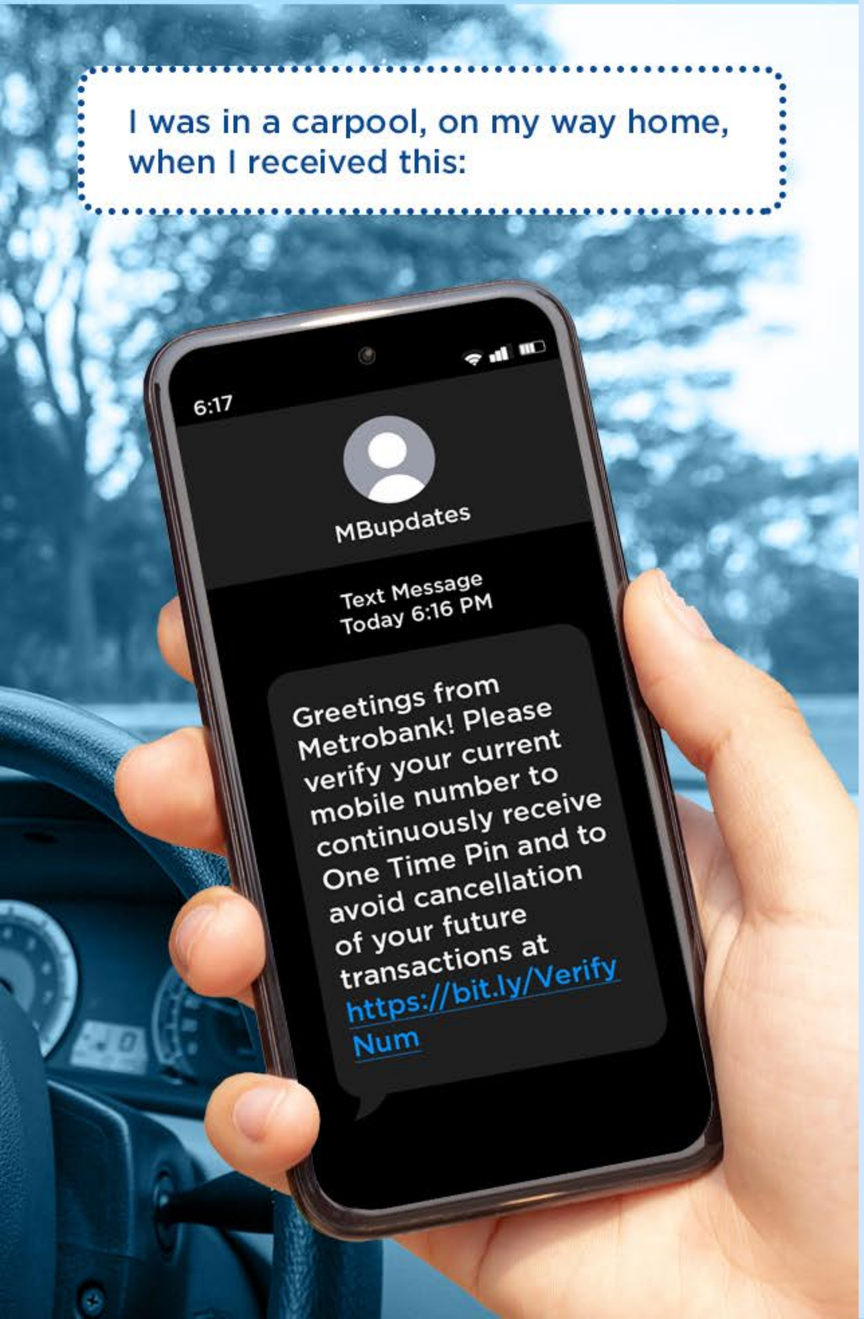
1. **Unknown Number**
2. **Fraudster introducing himself as someone from the LGU, DOH, DSWD, etc.**
3. **Fraudster using your basic personal information to appear legitimate**
4. **Asking to confirm personal information, bank details, and 6-digit OTP**

"I quickly blocked the number and asked my family and friends to do so as well."

ANTI-SCAM TIPS BY SAM

1. Be skeptical when receiving calls from unknown numbers.
2. Keep calm and ask for the caller's name, company and contact number, so you can report him later on.
3. Hang up the phone after getting the caller's details.
4. Never share your personal and bank information, including OTP.
5. Verify programs/ guidelines with your local government.

I was in a carpool, on my way home, when I received this:



"Wait, this a Smishing attempt! I can see some big RED FLAGS!"

RED FLAGS

1. **Sender is not the official account name of the bank**
2. **Contains suspicious links**
3. **Urgently asking to validate information like your mobile number, login credentials, OTP, etc.**

"I almost believed that Smishing attempt! I should always remember these red flags before doing anything."

ANTI-SCAM TIPS BY SAM

1. Never click on unverified links.
2. Never reveal your login credentials, mobile number, account number, OTP and CVV or Card Verification Value which is the 3 digit code on the back of your debit or credit card.
3. Do not respond to smishing attempts even if you know it's a scam. Replying confirms the validity of your contact number that may lead to future attacks.

Money Mule

I was looking for work online when I got a message to take a call at that very moment.

"So many RED FLAGS during that Saturday 7am call!"

RED FLAGS

1. They are immediately hiring without asking for educational background, skills or experience
2. No specific duties were mentioned
3. Immediately asking for a photo of a valid I.D. and complete personal details
4. Communication is awkward and has typographical and/ or grammar errors
5. Asking for my bank details or requiring me to immediately open an account where money will be deposited

"A monthly compensation for merely opening a bank account? They want to use me as a money mule!"

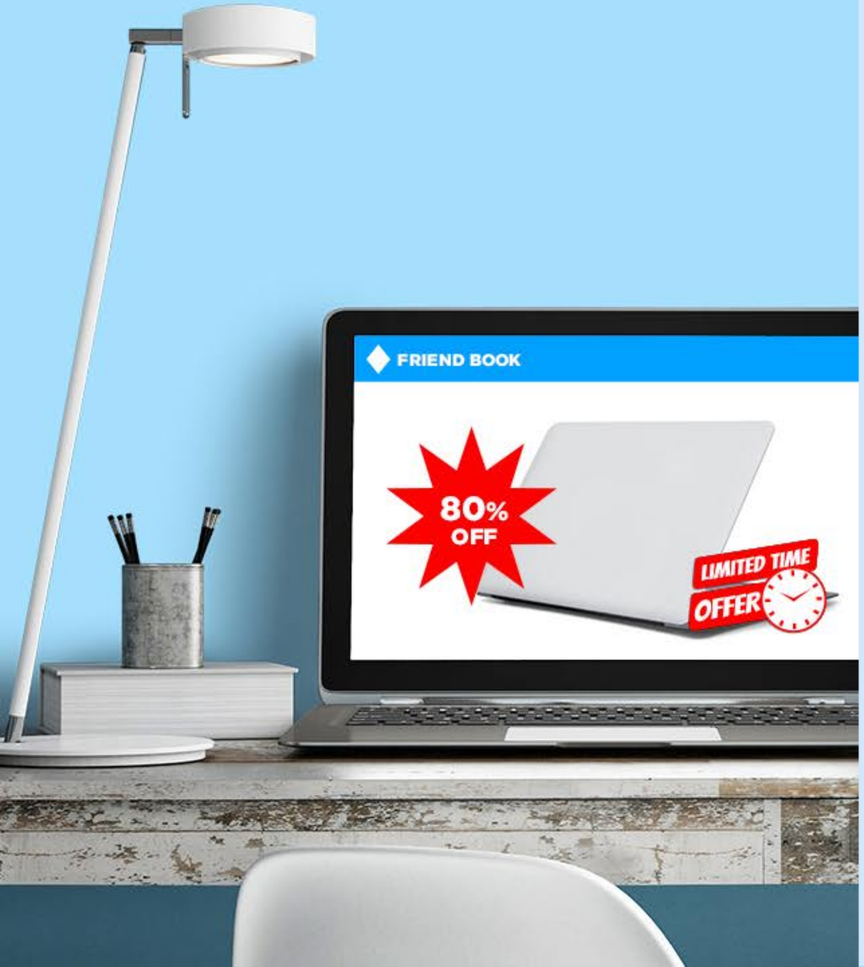
ANTI-SCAM TIPS BY SAM

1. Check legitimacy of work-from-home job offers.
2. Be extra wary of overseas job offers, since it will be harder to confirm if the company is legitimate.
3. No legitimate company will ask you to use your own bank account to transfer their money.
4. Do not give your bank, card or financial details to others. You are responsible for the transactions initiated from your card or bank account that you shared with, lent or sold to someone else.

Facilitating illegal money transfers is punishable under Republic Act No. 9160, Anti-Money Laundering Act of 2001 (AMLA), as amended, by imprisonment of up to seven years and fine of up to Php 3 million.

Online Discount Scam

I was shopping online when I saw this: a brand new laptop that's 80% off! What?!? That's a steal!



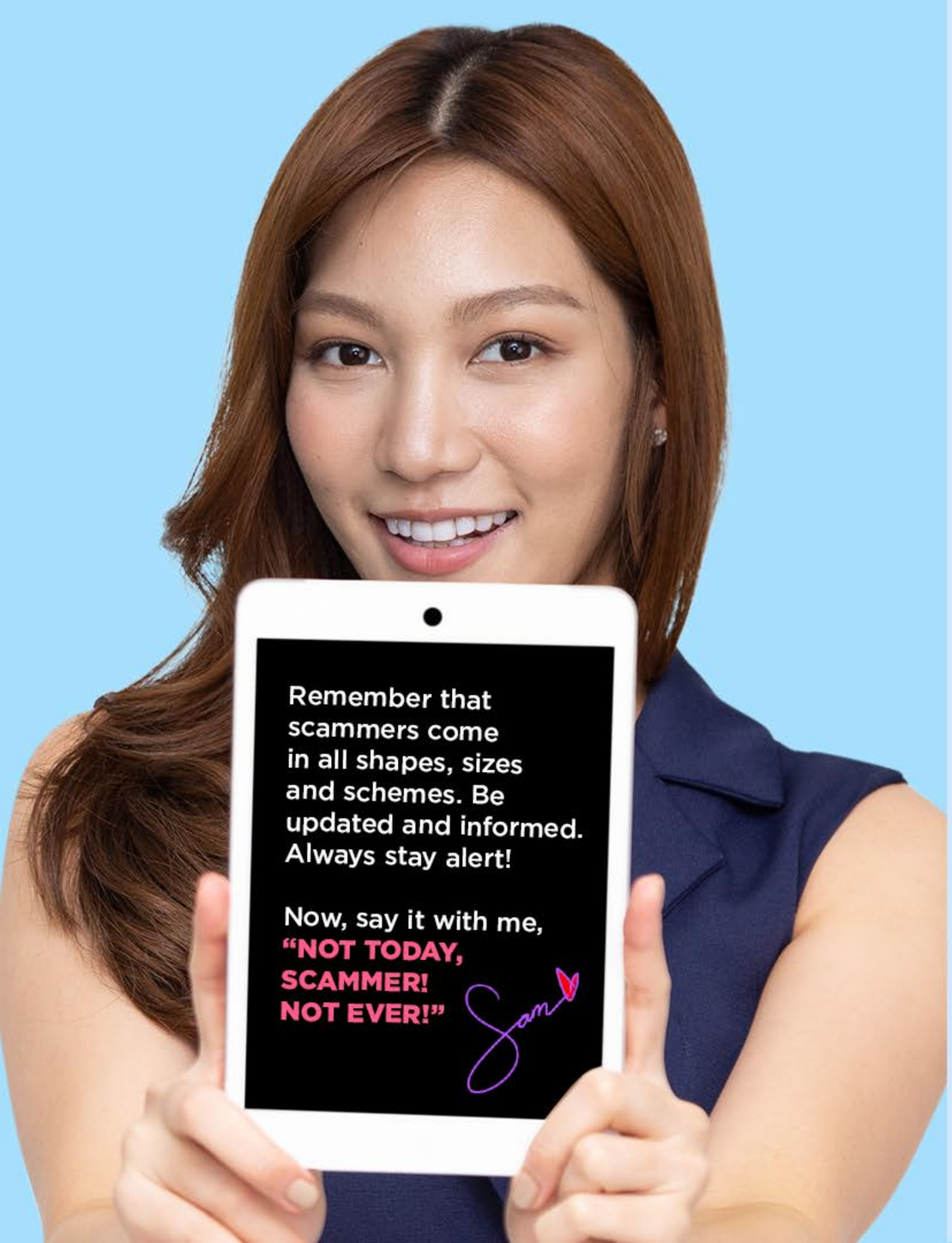
"Oh no! This looked exactly like the scam where my friend lost money! It's an online discount scam!"

RED FLAGS

1. Offers are too good to be true and are available for a limited time only
2. No reviews on the product
3. No company details on Facebook or in any redirected websites
4. No information on delivery and return policies
5. Requires immediate payment, but does not allow payment through secured channels

ANTI-SCAM TIPS BY SAM

1. Never click or download files from unknown and unsolicited sources. This may contain malware.
2. Do not make down payments until you confirmed the legitimacy of the online seller.
3. Be wary of sites asking for your personal or financial information.
4. Buy only from secure and reputable websites that start with **https://** and has a closed padlock symbol that reveals more info.
5. Transact only with 3D secure compliant merchants.
6. Opt for Cash on Delivery.
7. Never provide the mobile number and email address you use for banking purposes.



When in doubt, validate requests and offers by sending us a message via Metrobank's official Facebook Messenger or **@Metrobank** Twitter account before you give out your information.

If you suspect fraud, call Metrobank Contact Center at **(02) 88-700-700, 1-800-1888-5775,** or email us at **customercare@metrobank.com.ph** using "Report on Possible Fraud" as subject.

Regulated by **Bangko Sentral ng Pilipinas** |
Tel. No: 8708-7087 |
Email Address: consumeraffairs@bsp.gov.ph.

Metrobank
You're in good hands