BANGKO SENTRAL NG PILIPINAS

PROTECT YOURSELF FROM FRAUD AND SCAMS

Stay alert to avoid being victimized

Fraudsters and scammers have become more and more creative and sophisticated in their attempts to gain access to your personal information and financial accounts.

By knowing these common types of frauds and scams, you will be able to protect yourself and your hard-earned money.

Say NO to SCAMS!

What is a Scam?

A fraudulent scheme typically committed to cheat a victim into giving money resulting in the victim's financial loss.

Article 1338 of the Civil Code of the Philippines states that there is fraud when, through insidious words or machinations of one of the contracting parties, the other is induced to enter into a contract which, without them, he would not have agreed to.

Insidious words or machinations refer to a deceitful scheme or plot with a fraudulent purpose. It can be done by concealment or omission of material facts.

How do Frauds Happen?

False Representation

Fraudsters usually pose as someone they are not. They prey on people's emotions to manipulate our human tendency to trust. They tell stories that either resonate to our sensitive side or to our desires and aspirations. Then they employ tactics to induce pressure.

Phantom Riches

Fraudsters promise the prospect of instant and guaranteed wealth. People tend to forget that "If something sounds too good to be true, it usually is a scam."

Social Consensus

To increase trust, fraudsters claim that others have already joined or contributed to a cause at hand, like an investment opportunity.

Source Credibility

To further build credibility, fraudsters claim to be affiliated with a reputable agency or claim to have a special expertise.

Things to Keep in Mind to Avoid Financial and Investment Scams...

Scammers are experts in manipulation and they will spend time earning your trust until you let your guard down. To avoid loss when faced with a scammer, exercise the following three activities:

Think

Before providing personal information or giving away money, take a moment to pause and think about the credibility of the person or company you are dealing with, the soundness of the information being provided, and the possible risks of a certain action.

Examine

When in doubt, do not rush into a decision. Scammers usually create a false sense of urgency. Examine the situation first and ask questions. Challenge the person you are talking to about the things and ideas that you are not sure of and are uncomfortable with.

Study

Give yourself time to study and get as much information from different sources. Consult other people who are familiar to you or who are experts on the issue at hand. You can also get information from credible agencies like government institutions or reputable private organizations.

Source: Securities and Exchange Commission
https://www.sec.gov.ph/investors-education-and-information/investment-scam-checklist/

Common Types of Fraud and Scam:

SKIMMING AND JACKPOTTING

Illegal installation of malicious hardware (e.g., scanner, camera, keypad overlay) or software in Automated Teller Machines (ATMs) or Point-of-Sale (POS) devices. The scanner copies information on the debit, credit, or ATM card while the camera captures Personal Identification Number (PIN). This enables hackers to create counterfeit cards and gain access to accounts.

Jackpotting happens when an illegally installed software gives hackers control over ATM functions.

Remember:

- Look out for unusual features or loose parts of an ATM or POS device.
- Cover the keypad when entering your PIN. Use ATMs in well-lit and well-guarded areas. Ensure that your debit, credit, or ATM card is equipped with a Europay, MasterCard, and Visa (EMV) chip.
- Do not let other people use your card or stand close by when you make transactions.
- When transacting with a merchant using a POS device, keep an eye on your card and the cashier.
- Regularly check your account balance and billing statements. Report unauthorized or suspicious transactions to your bank or financial institution immediately.

Common Types of Fraud and Scam:

CARD CLONING

Creation of counterfeit credit, debit, or ATM cards, and using the same to make purchases or withdrawals against the legitimate owner's accounts.

Remember:

- Keep an eye on your cards at all times during all transactions.
- Do not post pictures of your cards on social media.
- Do not give your personal information and account details to anyone.
- Verify legitimacy of stores (including online shops) and their personnel.

Common Types of Fraud and Scam:

IDENTITY THEFT

A scammer assumes your identity and uses your personal information, bank account or credit card details to make unauthorized transactions and purchases, whether online or in person. They usually obtain a victim's personal information by posing as someone from an authority (like a bank or government office) and telling the victim that they need to provide personal information for official purposes. The same information can also be obtained through other fraudulent means like skimming, card cloning, phishing, vishing, and spoofing.

THEFT
of victim's personal and account information

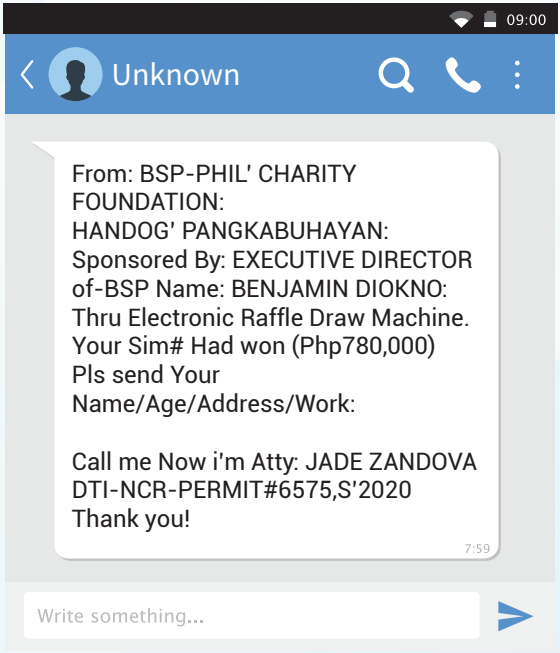
FRAUD
committed using stolen information to access victim's account

Remember:

- Beware of unexpected calls from someone claiming to be from position of authority and asking for personal information and bank details.
- Note down the person's details such as name, company and department. Always call your bank or financial institution directly to verify if the person is legitimate.
- Activate multi-factor authentication such as One-Time Password (OTP), security questions, biometrics, email and text alerts to get notified every time there is a transaction involving your accounts and cards.
- Safeguard your identification cards, bank statements, and billing statements.
- Immediately report incidences of identity theft, skimming, cloning, phishing, vishing, and spoofing to your bank or financial institution.

Common Types of Fraud and Scam:
TEXT SCAM

Random text messages asking for personal information, bank account or credit card details, or fees in exchange for an item or a service. Text scams come in many forms. Common text scams include winning a raffle you did not join and asking you to pay a shipping fee in order to receive the prize, requesting return of mistaken fund transfers to your account or phone, forcing you to pay for COVID-19 testing, or charging you for a service you did not avail of.



Remember:

- Always be cautious when dealing with unexpected text messages from strangers or random people.
- Verify their identities by asking for ID cards. Confirm their claims by directly calling the company they work for.
- Do not be pressured by anyone to share personal information; give money or pay a fee for unsolicited services.

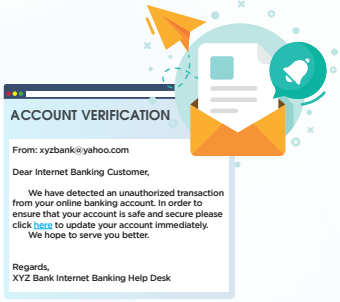
Common Types of Fraud and Scam:
PHISHING

Unexpected emails asking for your personal information, bank account or credit card details, or passwords. These emails usually ask you to click a link to a spoofed or fake website to enter your information. The email looks legitimate but often has a generic greeting (e.g., "Dear Valued Client"), grammatical errors, sense of urgency, and no verifiable contact information of the sender.

Remember:

- Do not provide personal information, account details, or passwords to senders of random emails.
- Your banks or financial institutions will never ask for such information through email. Do not click links or attachments in these emails.
- Always call your bank or financial institution directly to verify if an email is legitimate.
- Your banks and financial institutions have your details on record from the time you opened an account. They will only ask for your personal information if you initiated the call to make an inquiry or transaction.
- Immediately report incidences of phishing, or its variations, to your bank or financial institution.

Variations of Phishing:



Spear Phishing

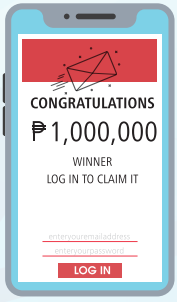
Sending of emails that are targeted attacks on specific individuals or companies.

Pharming

Redirection of a user to a fake website to steal personal information or account information details.

Vishing

Voice calls, automated voice recording, or Voice over Internet Protocol (VoIP) from someone pretending to be an employee of a bank or popular company, and asking for account details.



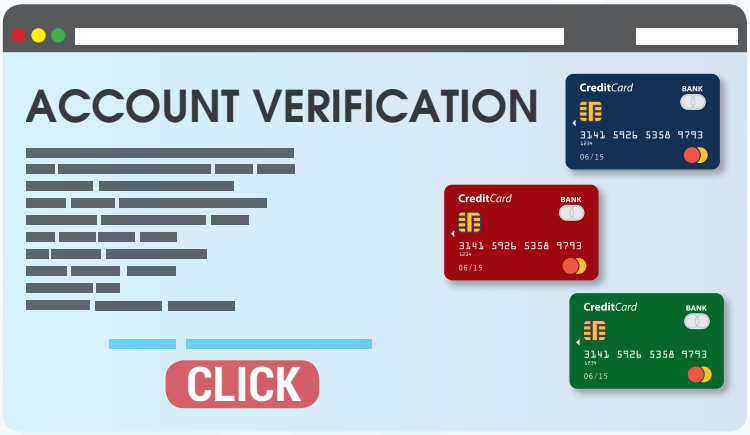
SMiShing

Same modus operandi as phishing but uses text or Short Message Service (SMS) on mobile phones instead of email.

Common Types of Fraud and Scam:

SPOOFED WEBSITES

Websites that look legitimate, but are created by scammers to trick you into entering personal information, bank account or credit card details. It is usually linked to phishing emails, or other fake websites.



Remember:

- Do not enter personal information, bank account or credit card details in suspicious or unverified websites.
- Always check the address bar or properties of a website to verify if it is legitimate.

How to check if website is legitimate:

Pay attention to the address bar

Check the website address for https:// at the beginning and a visible closed padlock icon (🔒). The "s" in https:// stands for "secure" and indicates that the website uses encryption to transfer data, protecting it from hackers. Do not enter personal information into a site beginning with http:// (without the "s").

Check the domain name

Be familiar with addresses and domain names of legitimate websites and type them directly on the address bar. Scammers create fake websites using addresses that mimic banks, popular brands, and companies. Double-check the address bar especially if you are redirected to it from another website or link.

Watch out for poor grammar and spelling

Mistakes in spelling, punctuation, capitalization, and grammar on a website are red flags. Legitimate companies put extra effort into creating a professional website free of such mistakes.

Try the contact information

Look for the company contact information (phone number, email, live chat, physical address) and try them out. You should hear professional customer service representatives or pre-recorded messages when calling a phone number. If the only method of contact is an email or an online form, proceed with caution.

Research before using a website

Do a quick online search of reviews of a website and look for warnings from reviewers or reliable organizations. You may verify the authenticity of a website through https://sitereview.bluecoat.com/# or https://www.virustotal.com/gui/home/url

Common Types of Fraud and Scam:
FAKE DOCUMENTS

Fraudulent documents allegedly serving as proof of peso or dollar deposit accounts, fund transfers, gold reserves, securities, or investments being marketed, sold or traded by individuals or companies which claim that such documents are issued, secured or guaranteed by the BSP, the government or any of its agencies.

BANGKO SENTRAL NG PILIPNAS
Pananalaping Matatag, Bansang Panatag
TREASURY DEPARTMENT
A. Mabini St., cor. P. Ocamo St., Malate Manila, Philippines 1004

FUND RELEASE ORDER

Date: 15/05/2018

Beneficiary Name: ABC FACTORY DISTRIBUTION INC.	**REMITTANCE ADVICE**
BANK NAME: XYZ BIRKENFELD	✓TRANSFER BY KEY TELEX
Bank Address: GERMANY	✓TELEGRAPHIC TRANSFER
Account Name: ABC FACTORY DISTRIBUTION INC.	RADIO MESSAGE
Swift Code: FAKERO	
Payment Ref: BSP/FAKE0034/2018	

AUTHORITY TO REMIT THE SUM OF $600,000.00

Sir,

As part of ensuring that the official mandate of the Treasury Department of the Bangko Sentral ng Pilipinas is carried out to effect the transfer of your due contract funds into your account, we have today keyed-in the sum of $600,000.00 in favor of ABC Factory Distribution Inc.

Thanks in anticipation for your promptness to enable us to serve you better.

Verified By:

Treasury Department Staff
Bangko Sentral ng Pilipinas

FAKE

TREASURY DEPARTMENT

DOC. SN-CIR-FMCA-RP-72

TO: CENTAL BANK DEF
Foreign Exchange Management

CC: AB and XY INVESTMENT CONSULTING COMPANY

DATE: 15 MAY 2018

Re: JUAN DELA CRUZ – XYZ BANK STOCKHOLDINGS ACCOUNT

Passbook Number:	9181 XYZ BANK PHILIPPINES
Passbook Name:	Juan Dela Cruz
Account Number:	12345678000
AMOUNT:	$5,045,000,000.00 United States Dollars
Date Issued:	November 31, 2010

GUARANTEE LETTER

SIR/MADAM,

WITH REFERENCE TO YOUR REQUEST, WE, THE BANGKO SENTRAL NG PILIPINAS IS CERTIFIED BASED ON RECORDS OF STOCKHOLDINGS DEPOSIT AND EQUIVALENT TO THE ACCOUNT OWNER, JUAN DELA CRUZ THE STOCKHOLDINGS CASH DEPOSIT AMOUNTING TO FIVE BILLION FORTY FIVE MILLION UNITED STATES DOLLORS (US$5,045,000,000.00).

WE HEREBY CONFIRM WITH FULL BANK RESPONSIBILITY THAT THE SAID FUNDS ARE CLEAN, CLEARED, LEGALLY EARNED, OF NON-CRIMINAL ORIGIN, WITHOUT LIEN AND ENCUMBRACES.

THIS GUARANTEE LETTER IS HIGHLY CONFIDENTIAL.

FOR AND ON BEHALF OF:
BANGKO SENTRAL NG PILIPINAS

GOVERNOR
BANGKO SENTRAL NG PILIPINAS
Pin# BSP-001GOV

FAKE

Remember:

- Do not believe any person or company claiming that possession of such documents can facilitate financial transactions in favor of holders or recipients.
- The BSP or government agencies do not authorize individuals or companies to market, sell or trade such items.
- The BSP in particular only deals with BSP Supervised Financial Institutions (BSFIs), institutional partners, and duly contracted suppliers of goods and services. The BSP does not provide banking and financial services to individuals and the general public.

Common Types of Fraud and Scam:

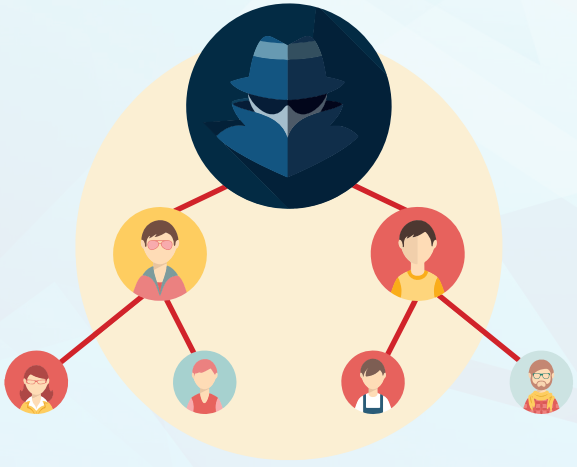
PONZI AND PYRAMIDING SCAM

Ponzi Scam

A scammer pretends to be a successful investment manager, owner or representative of a bogus investment company, or head or member of a reputable organization but, in reality, does not have an existing investment portfolio. The scammer would offer high returns in a short period of time, promising guaranteed profits with little or no risk of loss. The scammer is usually a skilled, charming, and convincing communicator who encourages investors to also invite others to invest and promises commissions for new recruits.

Pyramiding

Scammers convince investors to buy an investment product, and promise high earnings over a short period. Investors are required to recruit other buyers as their earnings increase based on the number of new recruits. Scammers normally pay investors back during the initial stages to appear legitimate and encourage more investors to buy the product. The "pyramid" eventually collapses when the money coming from new investors is not enough to cover the payouts to earlier investors.



Remember:

- Investment offers that sound "too good to be true" are usually scams.
- Even legitimate investment companies cannot double or triple your money over a short period of time and can never guarantee returns.
- Real investments are subject to the risk-return principle: The higher the expected return, the higher the potential risks.
- Do your own research about an investment company, its investment products, and authorized brokers or representatives.
- Do not engage in an investment opportunity if you do not fully understand how it works, how it earns, nor its risks and benefits.
- Do not let anyone pressure you into putting your hard-earned money into an investment opportunity.
- Always get and keep appropriate binding documentation and proofs (physical or digital forms) of your investments.
- Verify with the Securities and Exchange Commission (SEC) whether the company is registered and licensed to offer investment products.
- Check with SEC whether the company representative is a licensed investment broker or dealer.
- Report suspicious companies, persons, and transactions to the SEC.

How to know if Multi-Level Marketing is a Scam?

CAUTION

If the answer to any of the following questions is NO, it might be a SCAM!

8-Point Test*:

1. Is there a product?
2. Are commissions paid on sale of products and not on registration/ entry fees?
3. Is the intent to sell a product not a position?
4. Is there no direct correlation between the number of recruits and compensation?
5. If recruitment were to be stopped today, will the participants still make money?
6. Is there a reasonable product return policy?
7. Do products have fair market value?
8. Is there a compelling reason to buy?

*Source: Direct Selling Association of the Philippines
https://www.dsap.ph/the-industry/

Common Types of Fraud and Scam:

ADVANCE FEE FRAUD

An email, fax, or letter from strangers which requires the victim to pay an "advance fee" before receiving a significant share of a large sum of money. The advance payment may be described as a processing fee, tax, commission, or incidental expense that will be repaid later. If a victim makes the payment, the fraudster either invents a series of further fees for the victim or simply disappears.

Advance fee fraud may involve urgent business transaction, inheritance or income windfall, emergency situation, sale of products or services, lottery winnings, or other similar unexpected opportunities.

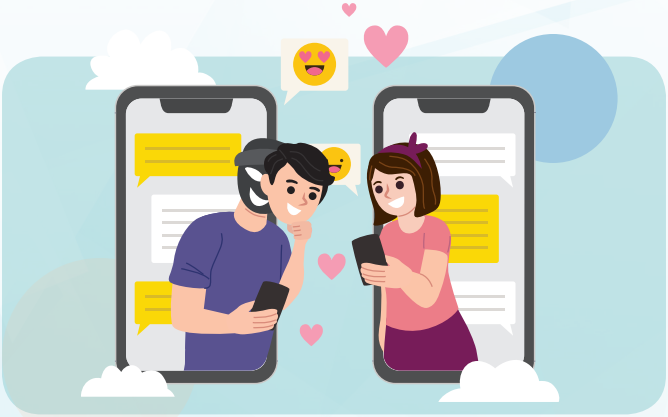
Remember:

- Avoid any arrangements with a stranger who asks for up-front and immediate payment, personal information, or account confirmation.
- Do not believe in offers or earning opportunities that are too good to be true.
- Do not send money, bank, and personal details to anyone you do not fully know or trust.

Common Types of Fraud and Scam:

ROMANCE AND DATING FRAUD

A scheme where scammers target the victim's emotional, romantic and compassionate side to get them to provide money, gifts, and personal or account information. Scammers target victims by creating fake profiles on social media or legitimate dating websites. Once in contact, the scammers will then express strong emotions for victims and will try to gain their trust and ask for money, account details and personal information for a variety of reasons (e.g., loss of job, involvement in accident or serious illness).



Remember:

- Think critically and remove the emotion from your decisions no matter how caring or persistent the person is.
- Avoid any arrangement with persons who ask for immediate payment or domestic or international fund transfers.
- Be careful about the information you share on social networking sites.
- Do not give your personal or bank details to strangers or acquaintances.
- Contact your bank or financial institution immediately if you think you have given out your account details to scammers or you feel that your account is compromised.

Common Types of Fraud and Scam:

RECRUITMENT FRAUD

Scammers pose as recruiters and offer fake job opportunities to obtain payments from job seekers. This is especially popular for supposed employment opportunities abroad. The scam starts with a fake job advertisement and then asks interested applicants for payment for various "requirements" like a certification, travel or work permit, and/or seminar fee. Once payment is done, the recruiter suddenly stops any communication.

Remember:

- Research the company advertising a job opening. Verify its legitimacy and ensure that the job opening actually exists.
- Check the legitimacy of the recruiter or company representative. Utilize available online resources like LinkedIn and other reputable job boards. Call the company to verify the credentials of the recruiter.
- Be cautious when asked for any upfront fees required to continue with the application.
- Do not share personal and bank information with the recruiter as this may lead to identity theft.

Common Types of Fraud and Scam:
SIM CARD FRAUD

Safeguard your Subscriber Identification Module (SIM) card!

Majority of banks and other financial institutions require Multi-Factor Authentication (MFA) in online transactions. This entails requiring customers to key in an OTP or password that they will receive via their registered mobile phone number, identified by a SIM card, before online transactions such as fund transfers can be completed. Fraudsters are therefore interested in this piece of information which is received on the victim's SIM card for them to carry out unauthorized fund transfers.

Attack Type 1:

Fraudster obtain personal and account details through phishing and other tactics. Once sufficient information is obtained, fraudster requests for a replacement of the victim's SIM card from the mobile phone provider. The old SIM is then deactivated by the mobile phone provider, allowing the fraudster to access the victim's accounts or make transactions since authentication verifications are now sent to the new SIM card in the possession of the fraudster.

Attack Type 2:

Fraudster in the guise of a telco representative entices the victim to exchange his/her SIM card for a fake “promo”. Once the victim agrees, the fraudster either clones or steals the victim's SIM card details and proceeds to access the victim's accounts for unauthorized transactions.

Remember:

- Never give out personal information and SIM card details in response to unsolicited call or texts from unknown or unverified individuals.
- Always check text and email alerts for unusual transactions or activities involving your accounts.
- In case you've already provided your SIM and other personal details, contact your bank/mobile phone provider immediately.

Common Types of Fraud and Scam:

UNAUTHORIZED ONLINE LENDERS

A scheme where fraudsters pretend as private individual lenders or claim to operate on behalf of a legitimate financial institution. They offer lenders credit lines or loans online, either through a website or social media platforms. Fraudsters will put more focus on collecting upfront fees for the so-called credit scoring or loan application and gathering the victim's personal details for potential or abusive fraudulent financial transactions.

Remember:

Before availing of a loan from a credit provider through a website or social media platform:

Do your research.

- Find out the registered name of the online lender, the company that provides the actual loan to online borrowers. Online lenders often use trade or brand names different from their registered or legal names.
- Understand the nature of the relationship between the online lender and the technology or platform provider or platform. Online lenders often partner with technology or platform provider, the company that enables a web-based interface to facilitate loan applications, but is not the actual lender.
- Check the online lender's track record and customer feedback. Look for red flags or warning signs of bad service and unfair practices.

Verify the online lender's licenses, registration, and authorization documents.

- Confirm that a BSFI—such as bank, pawnshop or e-money issuer that uses an online platform to provide loans—is licensed and authorized by the BSP. Search its name from the list of BSFIs on the BSP website, call the BSP Consumer Protection and Market Conduct Office, or chat with the BSP Online Buddy (BOB).

- Confirm that an online lender—such as a financing company or lending company is registered and authorized by the SEC. Check the SEC website regularly for advisories on unauthorized lenders or call the SEC to report unauthorized online lenders.

- Remember that you have no protection or recourse when you transact with unauthorized online lenders.

Follow these basic tips to protect yourself.

- Transact only with a duly licensed, registered, or authorized online lender.

- Transact only if you fully trust the online lender, its technology or platform provider and other partners, if any.

- Share personal and account information only if you have proven the integrity and security of the online lending platform.

- Borrow only if you have fully evaluated your credit needs, calculated your amortization, and assessed your capacity to pay the loan in full and on time.

- Borrow only if you have read and understood all the loan terms and conditions including interest rates, fees, and other charges.

- Keep proofs of transactions such as loan agreements, official receipts, confirmation of payments, and related communications.

- Make sure that the online lender has an accessible and effective consumer assistance or redress mechanism.

WHAT TO DO IF YOU GET SCAMMED:

Report frauds, scams, and abuses relating to products and services of BSFIs* to:

BSP Online Buddy (BOB)

Webchat
1. Go to https://www.bsp.gov.ph
2. Look for BOB's icon on the lower right portion of the page.
3. Click BOB's icon and a chat box will appear.

Facebook Messenger
1. Open the official BSP Facebook page
2. Click the Messenger icon
3. Click "Get Started"

SMS
1. Open your messaging app.
2. Text "Complaint" to 21582277 (For Globe subscribers only. Regular rates may apply).
3. Wait for acknowledgement and feedback prompt.

Bangko Sentral Ng Pilipinas
A. Mabini Street, Malate, Manila 1004

Consumer Protection and Market Conduct Office
Strategic Communication and Advocacy
Email: consumeraffairs@bsp.gov.ph
Direct Line: (02) 5306-2584 | (02) 8708-7087
Trunkline: (02) 8708-7701 loc. 2584
Facsimile: (02) 8708-7088

*BSFIs refer to Banks, Non-Banks with Quasi-Banking Functions, Non-Stock Savings and Loan Associations, Pawnshops, Foreign Exchange Dealers, Money Changers, Remittance Agents, E-Money Issuers, Money Service Businesses, and Virtual Currency Exchanges under BSP supervision. List of BSFIs may be accessed at https://www.bsp.gov.ph/SitePages/FinancialStability/Directories.aspx

WHAT TO DO IF YOU GET SCAMMED:

Report fraud, scams and abuses related to lending and investment with SEC-registered companies:

Securities and Exchange Commission PHILIPPINES

SECURITIES AND EXCHANGE COMMISSION
Ground Floor, North Wing Hall, Secretariat Building
PICC Complex, Vicente Sotto Street, Pasay City 1307

Corporate Governance and Finance Department
(Reports related to Lending)
Email: cgfd_md@sec.gov.ph
SEC i-Messagemo: http://imessagemo.sec.gov.ph
Telephone: (02) 8818 5476; (+63) 9260170248

Enforcement and Investor Protection Department
(Reports related to Investment Scams)
Email: epd@sec.gov.ph
Telephone: (02) 8818-6337; (+63) 961-519-7829;
(+63) 961-684-4088

Report concerns about insurance products to:

INSURANCE COMMISSION
1071 United Nations Avenue, Manila

Public Assistance and Mediation Division
Email: publicassistance@insurance.gov.ph
reportscam@insurance.gov.ph
Telephone: (02) 8523 8461 to 70 local 103 or 127;
(02) 8404 1758

WHAT TO DO IF YOU GET SCAMMED:

Report investment scams, cybercrime, and other criminal abuses to:

NATIONAL BUREAU OF INVESTIGATION
NBI Building, Taft Avenue, Ermita, Manila

Anti-Fraud and Action Division
Email: afad@nbi.gov.ph
Telephone: (02) 8523 8231 to 38 local 3529 or 3456

Cyber Crime Division
Email: ccd@nbi.gov.ph
Telephone: (02) 8523 8231 to 38 local 3455; (02) 8252-6228

Complaint and Recording Division
Telephone: (02) 8523-8231 to 38 local 3518

PHILIPPINE NATIONAL POLICE
Anti-Cybercrime Group
PNP National Headquarters
Camp General Crame, EDSA, Quezon City
Email: acg@pnp.gov.ph
Telephone: (02) 3414 1560
Mobile: 0998 598 8116

WHAT TO DO IF YOU GET SCAMMED:

To block text scammers, contact your phone service provider or report to:

NATIONAL TELECOMMUNICATIONS COMMISSION
NCR office address: BIR Road, East Triangle, Diliman, Quezon City

Consumer Welfare & Protection Division
Email: consumer@ntc.gov.ph
Telephone: (02) 8920 4464; (02) 8926 7722; (02) 8921 3251

ATM	Automated Teller Machine
BSP	Bangko Sentral ng Pilipinas
BOB	BSP Online Buddy
BSFI	BSP Supervised Financial Institution
DSAP	Direct Selling Association of the Philippines
EMV	Europay, MasterCard, and Visa
MFA	Multi-Factor Authentication
IP	Internet Protocol
OTP	One Time PIN
PIN	Personal Identification Number
POS	Point-of-Sale
SEC	Securities and Exchange Commission
SIM	Subscriber Identification Module
SMS	Short Message Service

BANGKO SENTRAL NG PILIPINAS
A. Mabini Street, Malate, Manila 1004

Consumer Protection and Market Conduct Office
Strategic Communication and Advocacy
Email: consumeraffairs@bsp.gov.ph
Direct Line: (02) 5306-2584 | (02) 8708-7087
Trunkline: (02) 8708-7701 loc. 2584
Facsimile: (02) 8708-7088