Holiday Scam

A rise in scams and theft usually occur during the holidays, so never let your guard down.

Stay alert against phishing and vishing:

- Watch out for calls and messages from unregistered numbers asking for your card details or One-Time Passcode (OTP) in exchange for rewards. Never provide these details to anyone.
- Don't open suspicious links sent via SMS from unknown numbers pretending to be a legitimate company.
- When in doubt, call the company hotline number listed in their official website to verify the request.

Make your online shopping safe:

- Check the URL to make sure you're on a legitimate and secure site. Keep an eye on poorly designed e-commerce sites.
- Verify if the seller is legitimate before finalizing the order by checking their reviews and customer feedback.
- Avoid sellers who post an advertisement under one name but ask the payment to be sent to a different name.
- Be careful of deals that seem too good to be true.
- Upon receiving your OTP, review the transaction details before completing your payment.
- Regularly review your card statement to spot any unauthorized transactions.

Keep your money and card secure:

- When investing or depositing money, hand over the cash to authorized personnel within the bank premises.
- Immediately sign at the back of your card upon receipt.
- Always secure your card and PINs. If you lost your card, report it to the bank immediately.
- When paying, always keep an eye on your card.
- Do not let other people use your card.
- Dispose of your card properly. Cut across the chip and throw away the pieces separately.

Providing your debit or credit card information or OTP to scammers, fake sellers, phishing websites, or losing your card may lead to fraudulent transactions that may be charged to you.