CONSUMER PROTECTION

WE'VE GOT **YOU** COVERED!

Can you spot an imposter scam?

An imposter is a person who pretends to be someone you know, the government, a company you do business with, debt collector, sweepstakes or lottery official, or a charity you trust. Imposters are dishonest people who want to steal your money or get your personal information. They might call you on the phone or send a letter, email or text. Imposters can try to get you to pay them by asking you to buy a gift card, use a payment app, or wire money. They could ask you to deposit a counterfeit check they provide. Never send money to people you don't know – especially if you cannot verify who they really are.

Common types of imposter scams include:

Government Scams: Government agencies, courts and law enforcement will contact you by mail, not by phone or email. Agencies will not ask for payment or seek personal information over the phone unless *you* initiate the call. Here are some tips to avoid government imposter scams:

- IRS will never call you and ask for money; it only communicates by mail.
- The police or sheriff's office does not take money directly for citations.
- ICE will not ask for personal information or a fee to unfreeze a shipment.
- Your SSN or Medicare ID has not been frozen due to fraud.

Scammers do their research and may use the real names of government agency employees. If you are concerned that you might owe fines or have missed jury duty or a court date, contact the agency or court directly, after locating the correct phone number online.

Known businesses: Imposters often mimic the logo, email or websites of well-known businesses or charities. Be wary of fraud or virus alerts, calls for unknown debts, lost shipment notices, sweepstakes or lottery awards, offers of prizes for survey responses, cold calls for unknown charities, and unsolicited messages asking you to click on links or open attachments. If you get calls, hang up and call the business or charity on a phone number you already had, or find on their official website. Tips to avoid business imposter scams include:

- Your bank may give you a pin to verify your account, but the caller may be a scammer on the other line with your bank posing as you. If you did not initiate the call with your bank, do

not give anyone the pin texted to you.
- Amazon will provide shipping updates on your account. Don't click on other texts or emails.
- Facebook isn't running a lottery; and if you did not enter, you did not win Publisher's Clearinghouse's or other sweepstakes.
- Microsoft and Apple have no idea if you have a virus on your computer.
- Costco, CVS, Walmart or Walgreens isn't sending you a free gift for a survey.
- If you don't have a Geek Squad membership, then the renewal message is false.
- Job scams often pose as a real business to get your SSN or money. Beware of interviews via Google Hangout, short interviews with quick hire decisions, and Gmail or other private emails where the business uses its own domain URL for its website.
- Beware of customer service scams by phone, email, mail or fake websites.

Friends & Family: Someone may contact you via email pretending to be a friend or family member who needs money because they are traveling and lost their wallet. Or they may claim to be calling on your sick grandchild's behalf for an emergency with someone crying in the background to heighten emotions. Red flags include when a new online love interest or friend you have never met in person asks you for money or offers investment advice, or when you hear from an unknown lawyer who represents an estate or inheritance for someone you do not know.

- Before sending any money or giving information, verify that your friend or family member is truly in distress by contacting them or another family member directly.
- If you haven't heard of this relative, much less their passing, you're likely not inheriting.
- Before giving money to an online friend for a secret "guaranteed" investment, or helping a romantic interest you met online financially, investigate who they really are.

Tips to avoid fraud:

1. Gift cards are for gifts. No legitimate business, government agency, or hospital will *demand* payment by gift cards.
2. Do not wire money or use a payment app to pay anyone who contacts you first.
3. Do not pay (whether by cash, check, gift card, payment app, or wire) until you have triple-checked the bill, the receiver, and the need to pay.
4. Do not give personal information to people who contact you first. The caller ID and the sender's email address can be faked.
5. If you didn't ask for the contact, or otherwise initiate the communication, be wary of a scam for money or personal information.

Howard County
Office of Consumer Protection

For more information on consumer topics, scan the QR code. To request this publication in an alternative format, contact the Howard County Office of Consumer Protection at 410-313-6420 or consumer@howardcountymd.gov.

SCAN ME