Brian E. Frosh
Attorney General

Media Contacts:
Press@oag.state.md.us
410-576-7009

Consumer Alert

Scam Alert: Phony Mortgage Company Representatives are Targeting Marylanders

The Office of the Attorney General has recently been notified of scams involving individuals impersonating mortgage companies. Some of these scammers are calling existing customers of a mortgage company, claiming to be representatives of that company, and offering the customer a loan modification. The scammer may ask for your full name, address, date of birth, and even your social security number. They may tell you that you have to give them this information immediately in order to qualify for the loan modification.

In another scam, individuals posing as mortgage company employees may call and tell you that you need to make a payment, and they may ask for a debit card number, money order, or gift card (this is a major red flag—no legitimate company will ask you to buy gift cards to make payments).

Other scammers may tell you to stop payment on your existing mortgage to make "trial" payments to them instead. They generally provide very "official" looking paperwork for you to sign. Do not fall for any of these tactics—they are trying to steal your personal information or money, or both. Under no circumstances should you ever stop payment on your mortgage. If you fail to pay your mortgage to the company that legitimately holds your loan, you could default on your loan and possibly even lose your home.

Telephone scams are common, and sometimes it can be difficult to distinguish legitimate calls from scammers. The caller ID could display the name of a real mortgage company in hopes they can trick you into answering the phone, but this is a common tactic used by scammers called "spoofing." If you do receive a phone call that displays the name of your mortgage company, our advice is to ignore the call and let it go to voicemail. Do not call back the number that was displayed on your phone. You can then call the company's actual phone number—listed on their official website—to ask if they called you and for what reason. If they did not call you, block the suspicious caller's phone number from trying to reach you again. Never give personal information to a caller you do not know or on a call you did not initiate.

If you have divulged personal or financial information to someone who called you, and now suspect they may have been trying to scam you, call or email our Identity Theft Unit at 410-576-6491 or idtheft@oag.state.md.us to learn how to protect your identity and financial information.