For Immediate Release - September 09, 2011

AG COAKLEY WARNS CONSUMERS OF WIDESPREAD "ROBO-CALLING" SCAM

Automated Phone Calls Seek To Gain Access To Consumers' Banking, Social Security Information

BOSTON - Attorney General Martha Coakley is warning consumers today about reports of a "robo-calling" scam that is seeking to gain access to consumers' banking and social security information.

"There are widespread reports from consumers who have received the automated phone calls asking people to enter their debit or credit card number," AG Coakley said. "We are warning people not to provide any personal banking information based on an automated phone call. If you receive one of these automated calls, you should immediately hang up and contact our consumer hotline."

Based on information and complaints received from consumers by the AG's Office and area banks, it is believed that the robo-calling scam began in early September. Bank customers, non-customers, and employees have received automated robo-calls typically between the hours of 11 p.m. and 6 a.m. These calls have frequently contacted consumers on their cell phones.

An example of a script of a typical call is as follows: "This is a call from NAME Bank. Your Mastercard account has been locked. Please press 1 now to unlock." The recording then instructs the individual to enter his or her debit card number in order to activate it. There have been additional reports that consumers are now being asked for their social security numbers.

Originating numbers for these phone calls include, but are not limited to:

· (508) 475-1394

· (214) 232-0615

· 1262 (just a four digit number)

· Many calls are from Unknown, Restricted, or Private numbers

If consumers receive one of these robo-calls, AG Coakley urges them to immediately hang up and contact the Attorney General's consumer hotline at 617-727-8400. Consumers are also encouraged to file a complaint with the office online at www.mass.gov/ago.

If consumers believe they may already be a victim of identity theft and have provided personal banking information or other personal information (e.g., Social Security number, credit card number) over the phone, AG Coakley offers the following advice:

1. Call one of the three major credit bureaus and place a one-call fraud alert on your credit report:

· Equifax: Call (800) 525-6285, www.equifax.com, or write: P.O. Box 740241, Atlanta, GA 30374-0241.

· Experian: Call (888) 397-3742, www.experian.com, or write: P.O. Box 9532, Allen, TX 75013.

· TransUnion: Call (800) 680-7289, www.transunion.com, or write: Fraud Victim Assistance Division, P.O. Box 6790 Fullerton, CA 92834-6790.

You only need to call one of the three credit bureaus; the one you contact is required by law to contact the other two credit bureaus. This one-call fraud alert will remain in your credit file for at least 90 days. The fraud alert requires creditors to contact you before opening any new accounts or increasing credit limits on your existing accounts. When you place a fraud alert on your credit report, you are entitled to order one free credit report from each of the three nationwide consumer reporting agencies.

2. Immediately examine your bank account for any suspicious activity. Whether you bank online or receive your statement in the mail, you may want to go over your statements with a fine toothed comb to ensure that there is nothing out of the ordinary on them. Report any irregularities to your financial institution.

3. Contact the fraud departments of your credit card issuers or bank. These financial institutions can monitor your account for suspicious activity. You may also wish to cancel these accounts; you can discuss this option with your credit card company or bank.

4. Order a copy of your credit report, and look for unauthorized activity. Look carefully for unexplained activity on your credit report.

5. If there is unexplained activity on your credit report, you may want to place an extended fraud alert on your credit report. If after reviewing your credit report you believe there is unexplained activity, you may want to place an extended fraud alert on your credit report. In order to do this, you need to file a police report with your local police department, keep a copy for yourself, and provide a copy to one of the three major credit bureaus. Then an extended fraud alert can be placed on your credit file for a 7-year period. This will mean that any time a user of your credit report (for instance, a credit company of lender) checks your credit report, it will be notified that you do not authorize any new credit cards, any increase in credit limits, the issuance of a new card on an existing account, or other increases in credit, unless the user takes extra precautions to ensure that it is giving the additional credit to you (and not to an identity thief).

####