## Do Not Call Registries

Register home and mobile phone numbers on the national Do Not Call Registry by visiting DoNotCall.gov, and register on the Florida Do Not Call List by visiting FDACS.gov/Consumer-Resources/Florida-Do-Not-Call.

Consumers can place their name and number on the federal Do Not Call list, and most legitimate companies will refrain from calling or texting those on the list. However, scammers and other illegitimate companies do not abide by the Do Not Call list, and consumers may still receive robotexts and calls after joining the list.

### Report Illegal Robocalls

Report unwanted robotexts or robocalls to the Florida Department of Agriculture and Consumer Services by visiting FDACS.gov/Consumer-Resources/Florida-Do-Not-Call.

Report scam messages to the Federal Trade Commission's Report Fraud website, ReportFraud.FTC.gov.

To report criminal activity involving malware related to robotexts or robocalls, contact the FBI's Internet Crime Complaint Center at IC3.gov.

You can also report scams associated with these messages to the Florida Attorney General's Office at MyFloridalegal.com.

## Florida Attorney General's Office Scams at a Glance:

## Robotexts and Robocalls

Visit MyFloridaLegal.com to find consumer tips or to file a complaint.

**Report fraud by calling**
**1-866-9-NO-SCAM**
**(1-866-966-7226)**

View other Scams at a Glance resources at:
MyFloridaLegal.com/ScamsAtAGlance

Office of the Attorney General
PL-01 The Capitol
Tallahassee, FL 32399-1050
MyFloridaLegal.com

Scams at a Glance:

# *Robotexts and Robocalls*

OFFICE OF ATTORNEY GENERAL

**JAMES UTHMEIER**

SAFE ★ STRONG ★ FREE

# What are Robotexts, Robocalls and Spoofing?

## Robotexts

Automated text messaging has grown more popular, with many companies using robotexts to communicate directly with consumers. Spam robotexts are now more prevalent than illegal robocalls. Robotexts are also used to transmit emergency information, such as inclement weather warnings, school closings and other pertinent information.

The Federal Communications Commission bans text messages sent to a mobile phone using an autodialer unless the consumer has given consent to receive the message, or the message is sent for emergency purposes. However, illegitimate companies and scammers tend not to heed these rules.

Spam robotexts are potentially more dangerous than robocalls because malicious links can be clicked on directly via text. Responding, liking or clicking on the contents of the text will show the scammer that the phone number is active, making the targeted user vulnerable to further messages.

## Robocalls

Robocalls are calls made with an autodialer, or contain a message made with an artificial or prerecorded voice.

Many legitimate companies use robocalls legally as part of their marketing or service operations; however, advances in technology have unfortunately allowed illegitimate companies and scammers to make illegal and spoofed robocalls easier than ever before.

In most circumstances for legitimate companies to use robocalls or robotexts legally, the Federal Communications Commission requires callers to obtain consent from a consumer, unless it is an emergency notification, and written consent if the call contains an advertisement or is telemarketing.

## Spoofing and Smishing

Caller ID spoofing is when a caller disguises the source of a call by falsifying the information transmitted to a user's caller ID. Spoofing is often used to attempt to trick a consumer into giving away valuable personal information for fraud or to be sold illegally.

Illegal robocallers will often use neighbor spoofing, which displays a phone number similar to the targeted user's own number, like using a target's area code, to increase the likelihood that the call is answered.

Smishing is a form of deceptive text messages intended to lure recipients into providing personal or financial information. These texts can be disguised as messages providing package tracking updates from shipping companies, or special deals and discounts from a trusted company. Clicking on the link in these illegal robotexts could install malware on the user's cellphone or could allow scammers access to personal information. Smishing also occurs under various schemes—so consumers should be cautious and never click on links in robotexts from unknown senders.

# How to Avoid Falling Victim to Robotext and Robocall Scams

## Robotexts:

- Avoid answering texts from unrecognized numbers. Responding to, liking or clicking these messages shows the scammer that the targeted user is active and will lead to more frequent scam messages.
- Do not click on links in text messages from unknown numbers as they often contain malware or lead to malicious websites.
- Consider downloading text and call blocking apps to further prevent these scam texts from reaching a mobile phone. Be sure to do research the apps before downloading to ensure that the app is legitimate.
- Know suspicious text messages from a five to six-digit short code telephone number may be a scam, unless the sender has registered the number in the U.S. Short Code Directory and the content of the message matches the registrant.

## Robocalls:

- Don't answer calls from unknown numbers —if the call is answered accidentally, hang up immediately.
- Never provide personal information, account numbers, Social Security numbers, passwords or other identifying information to unexpected or unsolicited calls.
- If a caller claims to represent a company or government agency and asks for personal information, hang up and call the phone number for the company or agency listed on an account statement or on the agency's website to verify the authenticity of the request.