From: Florida Department of Agriculture and Consumer Services
To: Florida Department of Agriculture and Consumer Services
Subject: Florida Consumer Newsletter - June 2019
Date: Wednesday, June 26, 2019 9:38:36 AM

Florida Department of Agriculture and Consumer Services

FCC AFFIRMS ROBOCALL BLOCKING BY DEFAULT TO HELP PROTECT CONSUMERS

Commission Also Seeks Comment on Requiring Caller ID Authentication Implementation & Use of Authentication Standards for Blocking

On June 6, 2019, the Federal Communications Commission voted to make clear that voice service providers **may aggressively block** unwanted robocalls before they reach consumers.

Specifically, the Commission approved a Declaratory Ruling to affirm that voice service providers may, as the default, block unwanted calls based on reasonable call analytics, as long as their customers are informed and have the opportunity to opt out of the blocking. **This action empowers providers to protect their customers from unwanted robocalls before those calls even reach the customers' phones**. While many phone companies now offer their customers call blocking tools on an opt-in basis, the Declaratory Ruling clarifies that they can provide them as the default, thus allowing them to protect more consumers from unwanted robocalls and making it more cost-effective to implement call blocking programs.

The ruling also clarifies that providers may offer their customers the choice to opt-in to tools that block calls from any number that does not appear on a customer's contact list or other "white lists." This option would allow consumers to decide directly whose calls they are willing to receive. Consumer white lists could be based on the customer's own contact list, updated automatically as consumers add and remove contacts from their smartphones.

The Commission also adopted a Notice of Proposed Rulemaking that proposes requiring voice service providers to implement the SHAKEN/STIR caller ID authentication framework, if major voice service providers fail to do so by the end of this year. It also seeks comment on whether the Commission should create a safe harbor for providers that block calls that are maliciously spoofed so that caller ID cannot be authenticated and that block calls that are "unsigned."

With adoption of this item, the Commission continues its multi-pronged strategy to combat unwanted and illegal robocalls. The Declaratory Ruling will go into effect upon release of the item on FCC.gov. The deadline for submitting comments in response to the Notice of Proposed Rulemaking will be established upon publication in the Federal Register.

Visit www.FCC.gov for more information on the Declaratory Ruling, the SHAKEN/STIR caller ID authentication framework, and combating spoofed robocalls.

JUNE IS NATIONAL INTERNET SAFETY MONTH

Kids and Online Safety

Summer is in full swing, and kids have even more free time to spend online. A 2018 Pew Research Center report shows that two-thirds of parents worry about their teen spending too much time online, and one-third worry a lot…and with good reason! Common Sense Media reported in 2018 that teens spend an average of nine hours a day online and kids eight to 12 spend about six hours.

Young kids should be supervised closely to ensure they don't stumble onto content that could scare or confuse them. Teens may seem sophisticated when it comes to using mobile devices or computers, but they still need guidance to help them understand which online sources are safe and trustworthy. Even the most tech-savvy kids need to be reminded that:

1. Not everything they see on the internet is true
2. People online may not be who they appear to be or say they are
3. Information or images they share can be seen around the world
4. Once something is posted online, it's all but impossible to take it back

The best way to protect kids online is to talk to them, early and often, about online safety. Kids are using smartphones and tablets at very young ages and need to begin learning the responsibilities and risks of the online world as soon as they are old enough to understand. Parents who communicate their values and expectations clearly can prepare their kids to make safe choices when confronted with tricky online situations.

Below are some tips to help ensure kids are practicing online safety:

- **Be positively engaged:** Pay attention to and know what sites your kids are visiting online.
- **Know the protection features of the websites and software your children use:** All major Internet service providers have tools to help you manage your child's online experience, e.g. selecting approved websites, monitoring the amount of time spent online, or limiting who can contact them.
- **Review privacy settings:** Decide which privacy settings on social networking sites, cell phones,

and other social tools are appropriate for your child's age and experience.

- **Explain the implications:** Help your child understand that anything they share on the internet can be easily copied and pasted elsewhere and is almost impossible to take back.
- **Stranger danger:** Help your child understand that not everyone is truthful about their identity online, and stress the importance of not sharing personal information
- **Be aware of all the ways your child can connect to the internet:** Phones, tablets, gaming systems, and even TVs can be connected to the Internet.

While it is extremely important to teach kids to look both ways before crossing the street and to be wary of strangers, it is equally important in today's world to teach them about online safety. Kids need guidance in determining what information should stay private and why. Finally, they should be encouraged to remember that real people with real feelings are behind the user names, profiles, and avatars of the people they encounter online.

Protecting Your Identity

Identity Theft Protection Tip: Beware of social media scams asking you to "verify your account."

In May 2019, it was revealed that Instagram's website leaked contact information of users over a four-month period. This information was gathered and stored on an unsecured database by the India-based marketing company Chtrbox. The data contained phone numbers and email addresses of individuals, businesses and even minors.

Unfortunately, there has been an increase in unprotected databases hosted online leaving many people with their information exposed without their knowledge. And, the more criminals find out about you, the more likely they can impersonate you or trick you into falling for a scam. With the increased frequency of data breaches and unprotected databases, it's important to always be on your toes.

While you can't do much about the unprotected databases, you can make sure you are doing everything in your power to minimize your risks. This includes being selective with what information you disclose online when signing up for social media accounts and always making sure your profiles is set to the highest privacy settings. It's also important to have strong passwords and change them often.

Visit the Identity Theft Resource Center for more information.

American Medical Collection Agency Reports Data Breach

The American Medical Collection Agency (AMCA), a third-party billing collections firm, recently notified medical testing giants LabCorp and Quest Diagnostics of a significant data breach. This breach exposed the personal, financial, and medical data of some 7.7 million LabCorp patients and almost 12 million Quest Diagnostics patients.

The breaches appear to have been first identified by Gemini Advisory (GA), a fraud intelligence and solutions firm. Approximately 200,000 patients' payment cards had been found by GA for sale on a well-known dark web market, and GA linked the cards to AMCA. GA reported their findings to law enforcement, who then contacted AMCA.

Financial identity theft and medical identity theft could both be a cause of the breach. Consumers who think they may be victims can start taking steps to minimize their risk. Resources for financial and medical identity theft and additional information regarding data breach can be found at www.idtheftcenter.org.

Individual Giving Survey

Provide valuable feedback regarding nonprofits and the causes, connections, and actions that lead to making a donation.

For less than 6 minutes of your time you can help to improve the process of giving for countless others.

Survey will close on August 15, 2019

VISIT US ONLINE AT

FLORIDACONSUMERHELP.COM AND

FLNONPROFITS.ORG/INDIVIDUALGIVINGSURVEY

CALL 1-800-435-7352 OR 1-800-352-9832 EN ESPAÑOL

Click to View Food Recalls

The Division of Food Safety monitors food from the point of manufacturing and distribution through wholesale and retail sales to ensure the public of safe, wholesome and properly represented food products.

Click to View Consumer Product Recalls

The Consumer Product Safety Commission provides consumer product recall information as part of the agency's mission to protect consumers and families from hazardous products.

The Florida Department of Agriculture and Consumer Services is the state's clearinghouse for consumer complaints, protection, and information. Consumers who believe fraud has taken place can contact the department's consumer protection and information hotline by calling 1-800-HELP-FLA (435-7352) or, for Spanish speakers, 1-800-FL-AYUDA (352-9832) or visit us online at FloridaConsumerHelp.com.

Follow us on Twitter -- @FDACS and @NikkiFriedFL

Florida Department of Agriculture and Consumer Services - Nicole Nikki Fried, Commissioner

You are subscribed to the Florida Consumer E-Newsletter. To change your email preferences, please point your browser to: http://www.freshfromflorida.com/Divisions-Offices/Consumer-Services/Consumer-E-Newsletter

Please do not reply to this message. It was generated from an account that isn't monitored, so replies to this email will not be read. You're welcome to get in touch with us through the Contact Us page of our website at www.FloridaConsumerHelp.com.

FDACS-P-00030 Rev. 06/19