Ohio Attorney General's
Consumer Advocate
Newsletter
JUNE 2017

SUMMER 2017

Know Your Rights: Robocalls

Federal laws generally prohibit companies from making robocalls to you without your written consent, so read on to learn more about the law and for tips to help limit future calls.

Robocalls use technology with either the ability to automatically dial phone numbers or to play messages using an artificial or pre-recorded voice.

The use of robocall technology has escalated drastically over the last 10 years due to the availability and use of internet-based telephone services, or voice-over-internet protocol (VoIP), such as Vonage. VoIP phone services are popular with consumers and telemarketers alike, due to their low costs and unlimited calling plans. Telemarketers using VoIP services can send hundreds of thousands of robocalls per day, limited only by the quality and speed of their internet connection. Many VoIP providers also allow their customers to choose the telephone number to display on the recipient's caller ID. This option allows scammers to fake, or "spoof," numbers to mask the true originating number and to change the number as frequently as desired to frustrate consumers' efforts to block the number.

The Telephone Consumer Protection Act (TCPA) addresses unwanted telephone solicitations, including restrictions on the delivery of "robocalls." Amendments to the TCPA, which became effective November 2015, tightened restrictions on robocalls by requiring callers to obtain certain permissions prior to calling.

Here is what you need to know about your TCPA rights:

- Calls and text messages have the same protections.
- All non-emergency robocalls, both telemarketing and informational, require a consumer's permission to be made to a wireless phone. These calls can include political, polling, and other non-telemarketing robocalls.
- Telemarketing (solicitation-to-purchase) robocalls to wireless and landline home phones require prior *written* consent from the recipient.

- Consumers can revoke their permission to be called or texted in any reasonable way. For example, a caller cannot require you to fill out a form and mail it in as the only way to revoke consent.
- Being an existing customer of a business does not constitute permission to be robocalled or texted.
- Callers are allowed to call a wrong number only once before updating their calling list. This most commonly comes up when consumers consent to be called or texted but then change phone numbers, leaving their prior number to be reassigned to someone else. Telemarketers and other callers have resources available to them to help them know ahead of time if a number's "owner" has changed.

Beware that many robocalls do not follow the TCPA or other telemarketing regulations.

Whether it's an automated call asking if you can hear, or a credit consolidation offer from "bank card services," don't take the bait. Hang up on any illegal or suspicious robocalls. Do not be tempted to follow a prompt to "press 1" to be removed from the calling list or to reach a live operator. Following the prompt by pressing a button only confirms for the sender that the call reached a live person. Unfortunately, that will only result in *more* unwanted calls to you.

To help reduce unwanted calls, follow these tips:

- Check out call-blocking services. Some mobile apps and cloud-based services combine data from reports of robocalls to create a "blacklist" of numbers that can be blocked from calling you.
- Visit www.donotcall.gov or call 888-382-1222 to register your landline or cellular number on the National Do Not Call Registry. If your number is on the registry and a company is still calling, there is a good chance it is a scam.
- Don't respond to suspicious calls in any way. Responding to a call could cause you to receive even more calls.

If you suspect a scam, contact the Ohio Attorney General's Office at 800-282-0515 or www.OhioProtects.org.

Five Free (or Low-Cost) Ways to Stop Identity Theft

Many identity theft protection services charge monthly or annual fees, but there are other free and low-cost methods to protect your identity.

Here are five ways to help safeguard your personal information, watch for warning signs, and limit damage caused by identity theft.

1. Checking your free annual credit report.

More than a decade ago, Congress passed a law allowing consumers to receive a free credit report from each of the three major credit reporting bureaus every year. Reviewing your credit report helps you understand what creditors can see about you and spot warning signs of identity theft.

To access your free annual credit reports, visit www.annualcreditreport.com, or call 877-322-8228. Some consumers choose a day they will remember (for example, their birthday) to request all three credit reports on the same date each year. Others choose to get a report from a different bureau every four months to regularly check for errors and signs of identity theft. For example, are there credit cards or loans listed that you never applied for? Are there loans or mortgages that are unfamiliar? If you find errors on a credit report, immediately notify the credit reporting bureau. The sooner you identify problems, the sooner you can work to correct them.

2. Placing an initial fraud alert on your credit report.

If you think you have had personal information compromised or if you receive a letter from a company or agency with which you do business informing you of a data breach, place an initial fraud alert on your credit report through one of the three credit reporting bureaus. Whichever agency you choose then is required to contact the other two bureaus. The alert, which lasts for 90 days, tells new creditors to check your identity if, for example, they receive an application for a new car loan or a new credit card using your personal information.

Below is the contact information for the three major credit reporting bureaus:

- Equifax, 800-525-6285, or www.equifax.com
- Experian, 888-397-3742, or www.experian.com
- TransUnion, 800-680-7289, or www.transunion.com

3. “Freezing” your credit.

Another – more permanent – step to consider is requesting a credit freeze. A credit freeze makes it harder for an imposter to open accounts using your personal information. Ohioans can freeze their credit report by contacting each of the credit reporting bureaus and paying $5 per bureau to place the freeze. (Parents and guardians also can freeze their child’s credit record to help prevent child identity theft.) A credit freeze is permanent unless or until the consumer lifts the freeze, which costs an additional $5 per bureau. The fee may be waived for victims of identity theft.

4. Safely disposing of documents.

Consider improving how you handle mail and other items that contain your personal information to safeguard your identity. If you simply throw such items in the trash, invest in a crosscut or confetti shredder so that dumpster-diving identity thieves will be less likely to steal your details and use them to open up credit cards or other accounts in your name. Buying a shredder can be a wise investment to protect your personal information.

5. Getting help from the Attorney General's Identity Theft Unit.

If someone obtains and uses your personal information without your permission to commit fraud, you are a victim of identity theft. The sooner you recognize the problem and take steps to correct it, the easier it generally will be to stop further damage. The Ohio Attorney General's Consumer Protection Section provides an Identity Theft Unit to help victims restore their identity. The Identity Theft Unit offers two programs, both of which are free to Ohio victims:

- Under the Traditional Assistance program, a consumer advocate will work with credit agencies, creditors, collectors, or other organizations on the victim's behalf. This option is ideal for those who are not comfortable trying to correct the effects of identity theft themselves.
- Under the Self-Help Assistance program, victims receive a step-by-step guide to attempt to rectify the effects of identity theft themselves. This option is ideal for those who prefer to work at their own pace and contact credit reporting agencies and creditors themselves.

If you are a victim of identity theft and need assistance, or if you suspect a scam or an unfair business practice, contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Taking the Mystery Out of Mystery Shopping

Mystery shopping jobs may appear to be flourishing, but make sure your secret shopper job doesn't become a surprise you never wanted. Learn to recognize the signs of mystery shopping scams and how to avoid falling for them.

People try to become mystery shoppers for a number of reasons. Some are looking for a career, while others are simply looking to supplement their income while maintaining flexible hours. In any case, it is vital that you know that many offers to be mystery shoppers are scams.

The mystery shopping scam has been stealing money and personal information from unsuspecting victims for years. The scam often begins when you answer an advertisement or unsolicited email to become a mystery shopper. The advertisement or email offers a job opportunity to shop at certain stores and then report on the experience for quality-control purposes. One reason the scam works is that there are real mystery shopping jobs. However, so many people are interested in this type of job opportunity that real mystery shopping companies generally do not send out unsolicited emails or advertise to hire people.

This spring, scammers contacted multiple Ohioans via email. The emails purported to be from "Kroger" and seemed authentic. They offered what appeared to be job opportunities as mystery shoppers and sought information from consumers who were interested. Consumers received checks ranging from $2,400 to $2,900 in the mail along with a letter instructing them to deposit the checks into their bank accounts. The consumers further were instructed to keep a small portion of the funds, and then send the bulk of the money to two other individuals via iTunes cards or via money orders sent from MoneyGram. Unfortunately, the checks were counterfeit, and the job opportunities were scams.

Mystery shopping scams often take advantage of the delay in time between when a check is deposited and when the bank discovers that it is counterfeit. In some cases, due to the high quality of the counterfeit check, it may take several weeks before a check is deemed counterfeit. At that time, the money is transferred, and the consumer is responsible for repaying the bank for the bounced check.

To avoid mystery shopping scams, be skeptical of companies that:

- Send you unsolicited emails or advertisements for mystery shopper jobs through the mail or email.
- Guarantee you work without a screening process.
- Send you money although you haven't worked.
- Make promises of large sums of fast cash.
- Demand money for signing you up as a shopper.
- Claim to be mystery shopping promoters who charge a fee for access to mystery shopping opportunities.
- Offer a certification or registration program for which you have to pay a fee.
- Advertise too-good-to-be-true salaries or benefits.
- Are located out of the country.

Finally, remember to never deposit a check for more than you are owed and then wire money back to the person sending you the check. Unlike credit card payments where you can get fraudulent payments erased or sending a check on which you can place a stop payment, wired funds and gift cards are irretrievable after they are sent. Unless you want an unintended surprise, never consider a payment you receive by check as being in your account until it has fully cleared the bank.

Consumers who suspect a scam or unfair business practice are encouraged to contact the Ohio Attorney General's Office by calling 800-282-0515 or visiting www.OhioProtects.org.

Crowdfunding: What to Know Before Donating

If you're asked to make a donation online to cover someone's medical costs, to help victims of a tragedy, or to fund another cause, learn the basics of crowdfunding and how to spot a potential scam.

Crowdfunding generally means funding a project through donations from a large number of people. It typically is conducted online, and in some cases, campaigns can go viral and quickly attract significant attention and money. A few common crowdfunding platforms include Kickstarter, Indiegogo, and GoFundMe, but an internet search of "crowdfunding sites" will reveal many more.

Crowdfunding can be used for various purposes. Charities may use it to collect donations, individuals may use it to raise money for medical costs or other needs, and businesses may use it to launch a new product or venture. Because there are many different types of crowdfunding sites and uses, it's important to gather as much information as possible before making a contribution.

Many crowdfunding campaigns attract money and attention to legitimate causes, but unfortunately, some accounts are scams designed to get your money or personal information. They may use names, photos, or details that sound legitimate, even though the donations will go to a scam artist.

To protect yourself, follow these tips:

- Never assume that fundraising recommendations on Facebook, blogs, or other websites have been approved or verified as legitimate. Research the opportunity yourself. Make sure you trust the person who has set up the fundraising page or account. Determine whether that person had permission (from the organization, individual, or family involved) to set up the account. Discuss the opportunity with people in the community to assess the need.
- Be vigilant when donating in the wake of a tragedy or natural disaster. Some people set up fundraising pages shortly after a tragic event in order to take advantage of the generosity of others. Even if someone sets up an account with good intentions, that person may not have the experience or knowledge to properly handle donations.
- Research charities and businesses using resources such as the Ohio Attorney General's Office, Better Business Bureau, IRS Select Check, Charity Navigator, GuideStar, Foundation Center, and Ohio Secretary of State.

- Understand that giving money to an individual or family is different from donating to an established charity. Your contribution may not be tax deductible. Before making a donation, ask whether the contribution is tax deductible, and verify it with your tax advisor or the IRS.
- Find out what percentage of your donation will go to the cause as opposed to the site or to the person who set up the account. Look for any additional fees that may apply to your contribution. Also find out whether there's a refund policy, what would happen if the raised funds fall short of the stated goal, and how the site handles complaints.
- Review privacy policies. Find out what the website will do (if anything) with your personal information. Be wary of websites that do not provide a privacy policy. Also, make sure the website is secure before entering your credit card number or other sensitive information. Look for the "https" in the web address; the "s" indicates that it's secure.

If you suspect an individual has set up a fraudulent account in order to steal money, notify the website where the account appears, and contact local law enforcement.

If you suspect a scam or unfair business practice, contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.