Ohio Attorney General's
Consumer Advocate
Newsletter
SEPTEMBER 2013

Beware of Insurance Enrollment Scams

While most consumers are familiar with the Affordable Care Act (ACA), commonly referred to as Obamacare, many are not aware of the specific procedures or important dates associated with the ACA. Fraudsters may use this lack of knowledge to scam consumers and possibly steal their identities.

In one variation of the scam, consumers may receive a call from a "licensed navigator." The caller will claim to be associated with the ACA and offer to help navigate the complex insurance enrollment process. However, in order to get started, the consumer must first provide personal information to "verify" his identity. In reality, the caller is not associated with the government. Consumers who provide any personal information increase their risk of fraud or identity theft. Open enrollment and legitimate marketing for insurance plans associated with the ACA will not begin until Oct. 1, 2013. Ohioans should contact the Ohio Health Insurance Marketplace for more information.

In another variation of the scam, consumers may receive a call from a "Medicare representative" claiming that the ACA requires seniors to obtain new Medicare cards immediately. The caller will claim that the senior must provide personal information in order to receive his new Medicare card. In reality, this is a scam. The ACA does not require seniors to obtain new Medicare cards. Consumers who receive a call such as this should not provide any personal information, should not mail in their current Medicare card, and should hang up the phone immediately.

The Ohio Department of Insurance (800-686-1526 and www.insurance.ohio.gov) has a wealth of information regarding the ACA, including Frequently Asked Questions for individuals, seniors, and employer.

Remember these tips to avoid ACA-related scams:

- On Oct. 1, 2013, Ohioans can get additional answers to their federal health insurance questions and begin the ACA enrollment process by visiting www.healthcare.gov or calling 800-318-2596.
- Legitimate government representatives will never contact you unexpectedly and request personal information such as your name, address, Medicare ID, Social Security number, or bank account information to begin the ACA enrollment process.
- Navigators are not permitted to steer consumers to a certain product, so if someone is steering you in one direction, it may be a scam.

If you suspect a scam or an unfair business practice, report it to the Ohio Attorney General's Office at www.OhioAttorneyGeneral.gov or 800-282-0515.

Don’t Bite on Phishing Schemes

In a typical phishing scam, a con artist pretends to be an employee of a bank or a government agency and asks for confirmation of account information by providing account numbers, passwords, or Social Security numbers. The scammer hopes consumers will fall for the scam and reveal personal information.

Recently, the Ohio Attorney General’s Office has received more complaints about phishing schemes. In one variation, a scammer calls a consumer and claims to represent a medical company. The “representative” informs the consumer that a medical supply order has been placed; however, personal information or a small amount of money is due to cover shipping charges. Consumers who reveal personal information or credit card numbers to cover the shipping increase their chances of identity theft or other fraud. For instance, providing credit card information for a $10 shipping fee allows the scammer to make more expensive charges to the card.

Similar to phishing schemes, robocalls also are used by scammers to obtain personal information. In a typical robocall, a consumer receives a phone call featuring a recorded voice. The recording prompts the consumer to press a button to learn more about a particular product or service. The recording claims that the consumer may press a different button in order to be placed on the company’s “Internal Do Not Call List.” By pressing either button, the consumer is confirming that their phone number is active. As a result, the consumer will continue to receive unwanted phone calls.

To avoid these types of scams:

- Maintain a record of products and/or services that you have ordered. If you receive a robocall, do not press any buttons. Hang up immediately.
- If the call is from someone with whom you do business, call them back at a number you are familiar with.
- Just as you would not give your personal information to a stranger who knocks on your door, never give your personal or credit card information over the phone to someone you do not know.
- In order to reduce unwanted phone calls, add your phone number to the https://www.donotcall.gov/ by calling the National Do Not Call Registry 888-382-1222.

If you suspect a phishing scam or an unfair business practice, report it to the Ohio Attorney General’s Office at www.OhioAttorneyGeneral.gov or 800-282-0515.

‘Mobile Wallet’ Security Tips

Smartphones and tablets allow consumers to stay connected, shop online, and even review bank account statements. Recent technology has taken convenience one step further, allowing consumers to use their smartphones as a mobile wallet.

A mobile wallet allows consumers to purchase products and services using one of many mobile apps available from credit card companies, technology companies, and individual merchants. Typically, the consumer links the wallet to a payment method such as a credit card or bank account. When shopping at a participating merchant, the purchase can be made simply by showing the wallet on the device at the cash register or providing the customer’s name.

Since personal information is required to use these applications, users should understand how information is stored and how to protect themselves against fraud. For example, consider this scenario: A consumer purchases an item using a mobile wallet or smartphone, which is set up to withdraw funds from a checking account. Later, the consumer misplaces the smartphone, which a thief finds and uses to tap into the mobile wallet. The thief is now able to use the consumer's phone to make fraudulent transactions.

Fortunately, there are a number of ways to protect personal information when using mobile wallet applications:

- Put a passcode on your smartphone. If your phone is lost or stolen, a passcode will make it harder for potential scammers to access your mobile wallet and personal information.
- Research mobile wallet applications before you download. Make sure that you fully understand all terms and conditions, including if the company you're considering sells personal information to other companies.
- Enable security features to protect your mobile devices, including the ability to track, lock, and erase information remotely in case they are lost or stolen.
- Update your mobile applications and software regularly.
- Avoid public Wi-Fi and only use secure networks when shopping online or logging into personal accounts.

If you suspect a scam or an unfair business practice, report it to the Ohio Attorney General's Office at www.OhioAttorneyGeneral.gov or by calling 800-282-0515.

AG Files Enforcement Actions Against Home Security Companies

Imagine a door-to-door solicitor pressuring you to purchase a home security system. He claims he can waive all installation fees and provide a 30-day right to cancel. However, after signing up, you notice unauthorized installation charges on your bank statements and unsuccessfully try to cancel the service. Similar situations have caused many consumers to file complaints with the Ohio Attorney General's Office.

In the past five months, the Ohio Attorney General's Office has resolved claims against three security companies: Platinum Protection LLC, Vivint Inc., and Vision Security LLC. The various actions involved alleged violations of the Ohio Consumer Sales Practices Act and the Home Solicitation Sales Act.

The Ohio Attorney General alleged that the prices on the contracts for monitoring fees were higher than the prices quoted verbally, that the companies failed to provide proper notification of consumers' three-day right to cancel, and that the companies failed to honor notices of cancellation when consumers quickly mailed, faxed, or delivered the notice to the companies.

Know your consumer rights before you encounter a door-to-door solicitor:

- In door-to-door sales of $25 or more, sellers must give consumers three days to cancel. The seller cannot install the product or perform any work within those three days.
- The seller must provide a written agreement and written cancellation notice. Make sure to read the contract and confirm that all of the verbal representations are accurately noted in the contract. If it's not in the contract, it does not become part of the agreement.

- If the consumer cancels the contract, the seller must provide a refund within 10 business days. Mondays through Saturdays count as business days. Sundays and federal holidays are not considered business days.

If you suspect a scam or unfair business practice, file a complaint with the Ohio Attorney General's Office at www.OhioAttorneyGeneral.gov or call 800-282-0515.