



Ohio Attorney General's
**Consumer Advocate
Newsletter**

AUGUST 2016

Ohio Consumers Gain New Law to Help Prevent Child ID Theft

Ohio families soon will have a new way to protect their children's identities. On June 29, Ohio Gov. John Kasich signed into law House Bill 317, which will allow parents or guardians to place a "freeze" on their child's credit record. The law takes effect on Sept. 28, 2016.

"This law will provide Ohio families with a new way to protect children from identity theft," said Ohio Attorney General Mike DeWine. "It will allow parents to freeze their child's credit record to stop identity thieves from opening accounts in the child's name. I thank all those who made this new protection possible, including Representative Ron Maag, who sponsored the bill, the Ohio General Assembly, and Governor John Kasich."

Representative Maag worked with Attorney General DeWine's Identity Theft Unit in the development of HB 317. Once effective, the law will require credit reporting agencies to both create and freeze a minor's credit record upon the request of the child's parent or guardian. The security freeze will help ensure that credit is not inappropriately granted in the minor's name, reducing the potential for identity theft. The new law also will allow the same protections for consumers over the age 16 for whom a guardian or conservator has been appointed.

In order to place a child security freeze, a parent or guardian must provide proof of authority to act on behalf of the child, such as a birth certificate, and proof of identity for both the child and the adult. The freeze will remain in effect unless it is lifted by the parent or by the child upon reaching the age of 16.

Currently, adults in Ohio already have the right to freeze their credit report. Typically, this is done by contacting each of the three major credit reporting agencies – Equifax, Experian, and TransUnion. The cost to place or to lift a security freeze may be up to \$5 each per agency. For victims of identity theft, the fee may be waived.

Once a security freeze is placed, the credit reporting agency will give the consumer a personal identification number (PIN) or password. Consumers must provide this PIN or password if they want to lift the freeze, either permanently or temporarily, such as when they're shopping for credit and need potential creditors to view their credit history. In Ohio, a security freeze is permanent unless or until it is lifted.

Adults who are concerned about identity theft but who don't want a permanent freeze on their credit report may want to request an initial fraud alert, which lasts for only 90 days. The fraud alert helps prevent others from being able to open accounts in a consumer's name and may be ideal for consumers whose information has been compromised in a data breach or whose information may have been accessed

inappropriately. To place an initial fraud alert, contact any one of the three major credit reporting agencies, which in turn must contact the other two.

If you believe you have been the victim of identity theft, contact the Ohio Attorney General's Office at 800-282-0515 or www.OhioProtects.org. The Attorney General's Identity Theft Unit helps consumers clear fraudulent debt and recover from the effects of identity theft.

Know Your Consumer Rights – Advertisements

Have you ever watched, read, or heard an advertisement and thought to yourself, “There’s got to be a catch,” or “This simply seems too good to be true”? Some ads may not tell the whole story. Some may even violate Ohio’s Consumer Sales Practices Act. In any case, understanding your rights as a consumer will help you avoid problems and make the most of your purchases.

The Consumer Sales Practices Act helps protect consumers from unfair and deceptive sales practices. It includes a number of advertising rules, such as:

1. ‘Bait-and-switch’ tactics are illegal.

Bait advertising occurs when an offer to sell a product or service is not a “good faith” offer. An offer may not be in good faith if it misrepresents an important aspect of the product or if the seller discourages the sale of the advertised product or service.

For example, imagine you see an advertisement for a great deal on a TV. When you go into the store, however, you find out that particular TV was never available for the advertised price, but the salesperson offers to sell you a similar TV that costs \$200 more than the advertised model. This is a classic case of “bait and switch.” Sellers cannot advertise one product only to get consumers to buy a different, higher-priced product.

2. Important exclusions and limitations of an offer must be listed.

If a sale includes any important limitations, those must be listed in the advertisement. For example, an ad should not indicate that all shoes are on sale if *only* children’s shoes are discounted. Advertisements also should list important terms, conditions, or extra costs that may affect the advertised offer. If the times of a sale are limited (“8 a.m. to noon only,” for example), then those hours also must be disclosed. If an ad includes a picture of items that are not included in the advertised price, this exclusion should be stated. All disclosures must be clear and conspicuous.

Let’s use the shoe sale for another example. Imagine a seller posts an ad offering “50 percent off shoes.” The ad includes the name of the seller but no other details. When customers go to make a purchase, they find out that in order to get 50 percent off their shoe purchase, they first must buy another pair of shoes at the regular price. Because all exclusions and limitations must be listed, the ad should have included the requirement that consumers buy one pair in order to get a second pair for 50 percent off.

3. ‘Free’ must really mean free.

A seller may not advertise goods as “free” when the cost of the “free” offer is passed on to the consumer by raising the regular price of the goods or services. For example, imagine a seller advertises a “buy one,

get one free” sale on a certain pair of shoes. If the regular price of the shoes is \$40, the seller may not raise the price of the shoes to \$80 during the sale only to offset the cost of the “free” item.

4. ‘New’ must really mean new.

Refurbished or reconditioned items may not be described as new and must be properly labeled as such. So if an electronics seller advertises a computer that has been used and refurbished, it should disclose the true condition to the consumer. (It should not advertise the computer as new.)

5. Price comparisons must be truthful.

A seller must not make misleading price comparisons that create false expectations in the minds of consumers. If an advertisement includes terms such as “discount,” “bargain,” “outlet,” “wholesale” or “factory prices,” the terms used must accurately describe the products offered for sale. For example, an ad should not indicate that TVs are “Regularly \$1,500, Now \$500,” unless \$1,500 actually is the regular price of the TV.

6. Terms and conditions of ‘prizes’ must be disclosed.

All important terms and conditions of a prize offer must be disclosed to consumers. For example, imagine you receive an ad saying you’ve won a beach vacation. If you are required to listen to a sales presentation in order to receive the beach vacation, the ad should notify you of that requirement.

Be sure to read future issues of the “Consumer Advocate” for more articles in the “Know Your Consumer Rights” series.

To report a scam or unfair business practice, contact the Ohio Attorney General’s Office by visiting www.OhioProtects.org or call 800-282-0515.

Searching for ‘Local’ Locksmiths May Lead to Faraway Call Centers

When consumers search for a locksmith, it is often when they need help in a crisis, such as being locked out of their own home or car. In a frantic search, they may not have the time, resources, or energy to thoroughly research a company’s reputation. But a little bit of checking may pay off, because some “local” locksmith ads actually lead to an out-of-area call center.

In one case, a Portland-area operation advertised under a variety of Ohio-sounding names, such as “247-locksmithcolumbus.com” and “daytonlocksmith.org.” When consumers called the phone numbers listed on the sites, however, their calls were transferred to an out-of-state call center, which then sent a referral to a contracted individual locksmith or locksmith company located in the community where the consumer lived.

Also, while consumers often were told the cost of picking the lock would be \$19, the actual price regularly turned out to be much higher, according to a lawsuit filed by the Ohio Attorney General’s Office against the operation. The lawsuit accused the defendants of misleading Ohio consumers and engaging in bait-and-switch practices.

To avoid locksmith problems, take steps to protect yourself, such as:

- Find a reputable locksmith before you need one. Ask family and friends for recommendations. Check for any complaints with the Ohio Attorney General's Office and Better Business Bureau.
- Be cautious of online ads for locksmiths. Research multiple businesses rather than selecting the first service you find online, and read online reviews of the company. Even if the locksmith uses a local-sounding website and phone number, don't assume the company is based locally.
- Be wary of businesses that operate under multiple business names. They could be using multiple names to hide unsatisfactory business practices from consumers.
- When a locksmith arrives at your home or vehicle, check the representative's identification. Be wary if the locksmith arrives in an unmarked car or has no official identification.
- Be skeptical if a locksmith says the only way to open the lock is to break it. Most skilled locksmiths can open locks without destroying them. Plus, breaking the lock could damage your property and result in much higher costs.
- Get an estimate from the company prior to having any work performed.

To report a scam or unfair business practice, contact the Ohio Attorney General's Office by visiting www.OhioProtects.org or calling 800-282-0515.

Five Signs of a Health Insurance Scam

Con artists know how complicated health insurance can be and are eager to take advantage of unsuspecting consumers. For example, while the Affordable Care Act, also known as "Obamacare," has been around for a few years, many consumers still have questions about it, and scammers may try to take advantage of the uncertainty.

Some consumers have filed complaints about calls from people claiming a connection to the Affordable Care Act or the Health Insurance Marketplace. One consumer from Ashtabula County complained about unsolicited phone calls from "National Health Enrollment" asking him for his insurance information. A Clermont County consumer received a call on his cell phone supposedly from the "Obamacare Enrollment Center." The caller told the consumer he needed to call back about his "registration," provided him with an "enrollment number," and wanted to discuss his enrollment and tax implications.

To protect yourself, watch for signs of a health insurance scam, including:

1. **Unexpected robocalls.** If you get a prerecorded sales call, or "robocall," it is probably illegal unless you have given written permission to get such a call. Some illegal robocalls are placed by scam artists hoping to get your money or personal information. Generally, the best way to handle such robocalls is to simply hang up. Do not push a button to speak to a live operator or to "opt-out" of receiving future calls. Pushing any buttons likely will result in more phone calls because it alerts callers that they have dialed a "live" telephone line.
2. **Requests for money.** If someone unexpectedly calls you claiming to be from the Health Insurance Marketplace and threatening to charge you penalties for not being properly insured, do not provide

personal information or pay money over the phone. Legitimate “Navigators” or trained “Assisters” of the Affordable Care Act should not charge you or try to sell you a specific plan.

3. **Copycat names.** Scammers often use names that are similar (or identical) to legitimate organizations. If you receive an unexpected call, letter, or other message about health insurance, check it carefully before responding. Don’t assume the message is from a legitimate source just because it includes an official-looking name or logo. The government provides information about the Health Insurance Marketplace at www.healthcare.gov; be cautious of lookalike names or websites.
4. **Requests to verify your personal information.** Be skeptical if you receive a health insurance call claiming to be from the government and asking for information. Legitimate organizations generally do not make phone calls to verify your personal information, such as your Social Security number. If you receive communication that appears to be official, contact the government office at a phone number you know to be legitimate in order to help determine whether the communication is part of a scam.
5. **Claims you need a new Medicare card.** If you are a senior on Medicare, you should not have to do anything new or different because of the Affordable Care Act. Do not trust someone who claims to be an insurance agent and tells you that you need that company’s policy or ID card to avoid a penalty or to keep access to your doctors. (Also, remember that your Social Security number is printed on your Medicare card, so think twice about carrying it around with you.)

To report a scam or unfair business practice, contact the Ohio Attorney General’s Office by visiting www.OhioProtects.org or calling 800-282-0515.