Ohio Attorney General's
Consumer Advocate
Newsletter
OCTOBER 2018

Federal Law Changes Can Help You Protect Your Identity – For Free!

Consumers often wonder how to best prevent identity theft before it happens. As of September 21, 2018, initial fraud alerts now last for one year and security freezes are free and available to adults and children.

Initial Fraud Alerts – An initial fraud alert mandates that a creditor takes additional steps to verify your identity prior to granting credit. For example, if you apply for an in-store credit card, the store may ask you to produce additional forms of identification or ask you questions that only you would know the answer to so that they can guarantee it is you. This can help protect your identity because the person pretending to be you would need multiple forms of identification or special knowledge to have credit granted in your name. Previously, initial fraud alerts stayed on a credit report for 90 days; that time has now increased to one year. For victims of identity fraud, an initial fraud alert will last seven years. You can continually renew initial fraud alerts after they expire.

Initial fraud alerts can be placed by contacting *any* one of the main credit reporting agencies (CRAs) – Equifax, Experian, or TransUnion; that company will then share the information with the other two CRAs.

Security Freezes - A security freeze restricts access to your credit report, resulting in most creditors refusing to grant new lines of credit unless the freeze is temporarily lifted or removed. Traditionally, in Ohio, CRAs could charge $5 each time a person added, lifted, or removed a security freeze. Now, the CRAs are prohibited from charging any fees associated with security freezes.

Security freezes can be placed by providing proper identification to *each* of the CRAs. After the first contact, the CRA has one day to place the freeze if requested via phone and three days after receipt of the request if placed via mail. To temporarily lift or permanently remove a security freeze, consumers must provide proof of identification, and the CRA must lift or remove the freeze within one hour if requested by phone, or online, or three days after receipt of the request if placed via mail. When requesting to temporarily lift a freeze, the consumer must specify when the freeze should be placed back on the credit report.

A "protected consumer" is a child under the age of 16 or a person for whom a guardian has been appointed. A parent/guardian can request a security freeze for that person so long as

they provide proof of authority to act on behalf of that person (ex. – court order, birth certificate, etc.) and proof of identification for the protected consumer and the parent/guardian (ex. – Social Security card for both). This freeze is also free of charge, and can be lifted later by the parent/guardian or by the child once the child turns 16 years old.

There are many ways to protect your identity. The initial fraud alert and the security freeze are both tools that are available under federal law, and the change in law now makes these tools free.

If you believe you have been the victim of identity theft, contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Take Action High School Video Contest Launches

Are you an Ohio high school student looking to earn scholarship money for college? Do you enjoy shooting and editing short videos? If so, put your creativity and consumer knowledge to the test for a chance to win up to $2,500 in college scholarships!

The Ohio Attorney General's Office and the Ohio Council on Economic Education encourage high school students to participate in the Take Action Video Contest. This special partnership seeks to raise awareness about important consumer topics students will encounter.

The contest officially began Sept. 10, 2018 but runs until Dec. 7, 2018. To participate, students (in teams of two or individually) should create a 60-second informational video on one of the following topics:

- National Do-Not-Call Registry
- Dealing with illegal robocalls
- Using technology to stop unwanted calls

The top three winning individuals or teams of two will be announced in March 2019 and will receive the following prizes:

- First place: $2,500 scholarship
- Second place: $1,500 scholarship
- Third place: $1,000 scholarship

To learn more, download the official 2018 Take Action Contest Guidelines. Teachers are encouraged to download the 2018 Take Action Contest Flyer to display in their schools.

Questions should be directed to the Ohio Attorney General's Office at 800-282-0515 or ConsumerOutreach@OhioAttorneyGeneral.gov.

Protect Your Apps: How to Make Your Smartphone More Secure

Your smartphone holds your favorite pictures, videos, and apps, but it also contains some of your most personal information. Hackers know this. During October's National Cybersecurity Awareness Month, learn several tips to make your smartphone more secure.

Consumers tend to overlook the fact that smartphones are miniature computers and are vulnerable to cyberattacks just like our home computers. On a phone, malware could expose your call logs, contacts, and usernames/passwords or could generate outbound calls and texts without your permission.

However, there are several simple ways to help protect you and your smart phone from cybercriminals:

- **Lock your phone.** This can be done by setting a PIN, pattern, or passcode in order to keep people from physically accessing your phone. While locking your phone won't protect you from online threats, it will keep your personal information safe if you lose your phone.
- **Limit the sites you visit while on unsecured Wi-Fi networks.** Hackers can monitor your activities when you're using unsecured Wi-Fi networks. Turn off the automatic Wi-Fi connection feature on your phone, and don't visit sensitive websites - like your bank – or enter payment card information while connected to public Wi-Fi.
- **Disable your device's Bluetooth capabilities.** When in public, disable your phone's Bluetooth capabilities. Bluetooth allows your phone to connect wirelessly with other electronic devices. Bluetooth could allow hackers to connect to your phone without your permission and put your personal information at risk.
- **Always verify apps before downloading.** When downloading apps, always use a legitimate app store such as Google Play or the App Store. Even then, malicious apps sometimes slip through the cracks. Before you download, look for too-good-to-be-true promises, bad or excessively positive reviews, and vague app permissions.
- **Use an antivirus app**. App stores are home to hundreds of antivirus programs. The National Cyber Security Alliance hosts staysafeonline.org where users can find a free "online security checkups and tools" section with antivirus suggestions.
- **Keep your phone operating system and all apps updated.** App makers and smartphone manufacturers are constantly putting together updates that help make your device more secure. Make sure your app and phone settings permit automatic security updates.
- **Before clicking, verify links found in text messages, multimedia messages, or emails.** Even if the message or email seems legitimate, always go directly to the website by specifically entering the web address into your internet browser. Never click on unknown links because they may contain malware.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Learn the Ten Signs of a Scam

Scammers use a variety of tactics to make their offers seem legitimate. Their initial contact may be by telephone, mail, door-to-door, flyers, emails, or phony websites. Be aware of ten signs that these initial contacts may be part of a bigger a scam.

- **Being asked to wire money or send a prepaid money card or gift card to a stranger or friend in need.**
  Scammers often use these payment methods because they are difficult to trace and tough for consumers to ever get their money back. Scammers may even ask you to simply read the numbers off the back of a gift card so that they can drain the money. Once the money is gone, it may be gone for good.
- **Pressure to "act now!"** Scammers don't want you to do your research or discuss the situation with a trusted friend or relative, so they devise tactics to rush you toward giving out your personal information and/or money immediately.
- **Requests for your personal information.** Be skeptical when asked for personal information. In general, if you are asked for more personal information than you feel is appropriate, ask them why they need it and how they will protect your information from being shared or stolen. Especially be on the lookout if you receive a cold call supposedly from a government agency such as the IRS.
- **Winning a contest you've never heard of or entered.** You cannot win a contest you did not enter. You cannot win a lottery unless you purchase a ticket. Never pay fees to win contests that you did not enter.
- **Suspicious Caller ID is displayed.** Using "spoofing" technology, scam artists can display any phone number they want on your Caller ID display. Those are likely from scammers who try to get you to answer their phone call by appearing to be from a local phone number. That's called "neighbor spoofing." They may also spoof the caller ID to appear to be from a legitimate agency or business.
- **Sending money in advance to secure a loan.** Scammers may try to convince you that you've been approved for a loan, but they need a payment in advance. If this happens, there's a good chance they will simply take your money and run. Never pay advanced fees to a stranger claiming they can guarantee your loan will be approved.
- **Requests for a large down payment.** Home improvement con artists are notorious for demanding large down payments because they want as much of your money up-front before doing an incomplete or shoddy job.
- **Being selected for a mystery shopping job, especially if you never applied.** While a few mystery shopping jobs are legitimate, many opportunities are cleverly devised scams using, again, wire transfers or prepaid gift card transactions. They may also

involve fake checks where you're asked to send money back to the scammer before the check clears.

- **A company that refuses to provide written information.** Be wary of any business that has nothing in writing to describe their company along with its products and services. Also, never consider any promised benefit as a guarantee unless it is in a contract signed by you and the business.
- **A company has no physical address, only a P.O. box.** Some scammers use P.O. boxes as the only address they give out to consumers. In reality, the box may simply be a collection point for the money they are stealing.

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.