Ohio Attorney General's
Consumer Advocate Newsletter
Keeping Consumers Safe and Informed

December 2020

What To Know About Giving Gift Cards

Gift cards are popular holiday presents, especially for last-minute shoppers and for recipients who don't have a wish list. Not all gift cards are alike, though. It's important to know some basics about them – from variable expiration dates to signs of potential scams – before you make such purchases.

Gift cards are protected under both state and federal law. Under Ohio law, gift cards in any form — electronic, paper, etc. — generally cannot expire for at least two years. Under federal law, gift cards issued in electronic format for a specific amount cannot expire for at least five years. Pay attention to a card's expiration date, especially if you are buying a gift card from a re-seller.

If a gift card has no expiration date, it is generally valid until redeemed or replaced with a new card. Still, it is often best to use a gift card as quickly as possible – to reduce the chance that it will be lost or stolen or that the business will close before you've used the card.

There are a number of exceptions related to gift card laws. For example, gift cards purchased for a specific service, such as a gift card for one manicure (as opposed to a specific dollar amount to a nail salon), are not protected under federal law. Additionally, "bonus" cards are not protected under state or federal law. During the holiday season, many businesses offer deals,

such as “buy a $100 gift card, get a $20 gift card free.” Although the $100 gift card would have all the protections the law offers, the $20 gift card would not – and it could expire at any time. Closely verify the expiration dates and other restrictions of any bonus cards.

Keep in mind that a reloadable gift card that can be used almost anywhere may reduce in value faster than a single-store gift card and is not required to have an expiration date in excess of two years from the date of purchase. Such cards may also impose a fee when the card is more than 2 years old and inactive for 12 months.

Gift cards are also frequently used in scams. For example, you may come across a legitimate-looking website advertising better deals than stores’ websites, but, at the checkout page, the website requests the number to a gift card (not associated with the company) instead of a credit or debit card. Beware! Scammers may create phony websites — complete with made-up customer reviews — to trick people into revealing redeemable gift card information. Unfortunately, once the information is provided, any money loaded on the card will be lost.

Similarly, a con artist may call you, claiming that you’re in trouble with the IRS or that someone you love needs help, and ask you to pay immediately using a gift card. This is a common sign of a scam. Once you provide the gift card information, even just by reading the gift card numbers over the phone, the con artists can drain the funds.

When you buy gift cards in a store, be sure that any PINs – generally located on the back of gift cards – are not already scratched off. Some scammers go into stores, scratch off and record PINs, and put the gift cards back on the shelf. Then they regularly check to see whether a consumer has purchased (or put any funds on) the card. The scammer then drains the card before you’ve had the chance to give or use the gift card.

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.

Watch Out For False Promises When Fulfilling New Year’s Resolutions

The beginning of a new year is traditionally the time for people to work toward a healthier lifestyle, but be sure to protect yourself as you seek to fulfill your resolutions.

If joining a fitness center is part of your plan, search complaints on file with the Ohio Attorney General’s Office and the local Better Business Bureau to determine whether customers have been satisfied with the gym’s services. Common complaints include fitness centers closing without notice, overcharging for services or not clearly explaining cancellation rights.

Typically, you will be asked to sign a contract when joining a gym. As with any other contract, you should read it completely to be sure that you understand all the terms and conditions and to ensure that any promises made by a salesperson are included in the contract.

Under Ohio law, gym membership contracts generally should not last longer than three years. Also, regardless of the gym's cancellation policy, Ohio law generally provides you three business days (excluding Sundays or legal holidays) to cancel your contract in full at no cost after an initial sign-up. Before signing the contract, ask about the facility's cancellation policy, and determine what your responsibilities are if you decide to end the contract early. This is especially important in the wake of COVID-19. Some gyms may continue to charge even if the gym is closed; others may not. Get those details in writing.

Also, look out for "negative option" contracts. Under such contracts, consumers are automatically re-enrolled at the end of their current contract and money is automatically charged. For example, a gym might automatically renew an annual membership by charging the consumer's credit card for the entire next year when the first year is about to expire. Such a policy makes it difficult for the consumer to remember to cancel the contract in time to avoid the new annual membership fee.

Dietary supplements also have become popular in the weight-loss industry and often are touted as a quick, easy solution to a difficult health problem. Although these supplements may be advertised as yielding fast results, you should take time to research products before trying them. Look online for reviews from others who have tried the product, detailing whether it worked for them, and check for any scientific research conducted on the product. Most important, keep in mind that some supplements have been shown to cause harmful side effects. To avoid potentially dangerous products, check with your doctor or other trusted health-care professional before making a purchase. Also, beware of any email or website claiming to have a vaccine or supplement to cure the COVID-19 virus.

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

Getting A New Device? Take Steps to Secure It and Stay Safe

As the holidays and a new year approach, plenty of Ohioans are looking forward to getting a new electronic device. What do you need to know before you start downloading apps? Plenty, including the red flags of a fake app as well as key parts of an app's privacy policies.

Fake apps look like legitimate apps and appear to function the same way that a legitimate app does – both done intentionally so that users are inclined to download them. Once you download a phony app, though, it might begin to steal your personal information, load malicious content on your device and/or aggressively display unwanted advertisements.

Here are some red flags to help you determine whether an app may be phony:

- Look for changes or misspellings in an app name and logo. Be sure to research the developer's name and the proper name of the app. Typically, you should even be able to click on the developer's name to find its other apps.

- Read app reviews for any problems that other users have identified with the app. A high number of negative comments could indicate that the app is fake or too risky to download until some of the kinks are resolved.
- Check the date of the app. Most popular apps have been out for a while, and you should see an “updated on” date instead of a publication date. If you see a very recent publication date, be sure you have chosen the correct app.
- Be leery of too-good-to-be-true discounts. If you see a bargain, remember that the developers of fake apps may use these promotional prices to lure you into downloading their fake apps.
- Look at the developer screenshots that are typically included in the app store to help you understand how the app functions. If the screenshots are Photoshop images or use words or taglines unusual to the developer, be careful. The app could be phony.
- Read the description of the app, again looking for misspellings or text possibly written by an automated robot instead of a human developer. Most legitimate developers thoroughly describe their app in language understandable to the average user.
- Look at the current number of downloads indicated. Popular apps are typically downloaded millions of times. A phony app may have, say, only 1,000 downloads.
- Review the permissions requested by the app to be fully functional. A fake app might request permissions that may be unnecessary or unrelated to the app. Always be concerned if the app requests permissions that make you uncomfortable.

For parents of children using a device, consider what parental controls you may be able to use or download to help ensure that your children’s activities and downloads are age-appropriate. Some controls may help keep your children safe and away from predators. Also, be aware that some scams occur through purchases made directly from the app (known as “in-app purchases”) after you download it. For parents, talk with your kids about watching out for “free” offers that may be costly scams, and consider blocking in-app purchases or making them password-protected so that your child makes no in-app purchases without your permission. You may also consider controlling the password needed to download apps so that you are aware of all apps downloaded by your child.

Reviewing an app’s privacy policy before supplying any personal information is another way to protect yourself. The privacy policy is where companies outline and justify why they collect and, depending on the company, might share or sell your personal information, as well as what the company does to try to protect your data.

Within the privacy policies, look for opportunities to “opt out” of sharing personal information with third parties for marketing purposes. Also, see whether the privacy policy allows you to delete or correct the personal information that it has gathered and stored. If you’re not comfortable with sharing your personal information as outlined in the privacy policy, question whether you really need the app on your device, or whether an alternative app might better suit your needs.

Protect Yourself From Identity Theft

Unfortunately, in today's world, the odds are pretty good that you or someone you know has been a victim of identity theft. The upside is that Ohioans can proactively take steps to help secure their personal information.

The Consumer Protection Section of the Ohio Attorney General's Office offers these tips to help you avoid falling victim to the crime of identity theft:

- Never share personal information with anyone who contacts you unexpectedly.
- Consider placing an initial fraud alert or a security freeze on your credit report (more on that below).
- Never carry unnecessary personal information, such as your Social Security card, in your wallet or purse.
- Shred all outdated documents containing personal information.
- Make copies of your credit cards, and store them securely so you can call to cancel them quickly if they go missing.
- If a bill fails to arrive, contact the company as soon as you notice its delay; thieves sometimes steal information from mailboxes or reroute others' bills.

For consumers using internet-connected devices at home, around town and/or while traveling:

- Don't conduct private business on public Wi-Fi.
- Regularly update your computer software and mobile apps.
- Use internet passwords that are long and difficult to guess, and change them regularly.
- Set a passcode on your smartphone.
- When entering personal information online, make sure a website is secure by looking for the "s" in "https."

Checking your credit report is also important in the fight against identity theft. Due to COVID-19, you are able to receive one free credit report **per week** from each of the three major credit-reporting agencies through April 2021. For details, visit www.AnnualCreditReport.com.

You may also wish to place an initial fraud alert or security freeze on your credit reports. The initial fraud alert will last for one year, can be canceled at any time and is renewable. An initial fraud alert can make it harder for an identity thief to open accounts in your name, and you should be notified if there are any attempts to open new accounts using your personal information. You need to contact only one of the three national credit-reporting agencies to place an alert; that agency then will contact the other two agencies. You may contact one of the following:

- TransUnion, www.transunion.com, 800-680-7289
- Equifax, www.equifax.com, 800-525-6285

- Experian, www.experian.com, 888-397-3742

You may also consider placing a security freeze on your credit reports. This prohibits a credit-reporting agency from releasing information on your credit report without your express authorization or approval. A credit freeze is designed to prevent an impostor from using your information to be approved for credit, loans or services in your name.

If you wish to freeze your credit with all three of the credit-reporting agencies, you must send a request to each agency. You can request a temporary lifting of the credit freeze at any time. There are no charges to place, temporarily lift or remove a credit freeze.

The Ohio Attorney General's Office has an Identity Theft Unit whose members help to rectify the effects of identity theft. A consumer advocate will work with credit agencies, creditors, collectors or other organizations on your behalf.

If you need assistance as an identity theft victim 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.