Attorney General's Consumer Holiday Guide

Wishing You a Safe Holiday Season!

Cynthia H. Coffman
Colorado Attorney General

STOP Fraud Colorado™

Message from Attorney General Cynthia H. Coffman

Merry Christmas, Feliz Navidad, Happy Hanukkah, and a Joyous New Year!

This time of year we gather with family and friends to celebrate the holidays and look ahead to a new year full of possibilities. It's a season when many of us share our holiday spirit by exchanging gifts and donating to charitable causes. Unfortunately, the holidays also can create opportunities for individuals who would take advantage of our generous natures.

The Attorney General's consumer protection team is hard at work all year long identifying unscrupulous business practices and educating Coloradans on topic like the latest scams and charity fraud, protection against identity theft, and steps to take if you suspect wrongdoing. The *Attorney General's Consumer Holiday Guide* includes tips and resources that will help ensure a trouble-free and happy holiday season. Please share the *Guide* with your friends and family and help spread the word on social media.

On behalf of the entire staff of the Colorado Attorney General's Office, I wish you and yours a Merry Christmas, Feliz Navidad, Happy Hanukkah, and a joyous New Year.

Cynthia H. Coffman

Colorado Attorney General
Cynthia H. Coffman

CHARITY FRAUD

These days, charities and paid solicitors (groups that solicit funds on behalf of organizations) use the phone, face-to-face contact, e-mail, the Internet (including social networking and crowd funding sites), and mobile devices to solicit and obtain donations.

But, how do you tell a legitimate charity from a fake one? Following are a few red flags that should lead you to at least question the legitimacy of a charity. See also the 2016 Colorado Charitable Giving Survey to better understand charitable giving behaviors at: **http://bit.ly/2016CharitableGivingSurvey**.

Red Flags of a Charity Scam:

Regardless of how you are reached, make sure to avoid any charity or fundraiser that refuses to provide detailed information about its identity, mission, costs, and how the donation will be used. Some other red flags are when a charity or its paid solicitor:

- Can't provide Colorado Secretary of State registration information;
- Won't provide proof that a contribution is tax deductible;
- Thanks you for a previous pledge you don't remember making;
- Uses high-pressure tactics, like trying to get you to donate immediately, without giving you time to think about it and do your research;
- Asks for donations in cash or asks you to wire money;
- Offers to send a courier or overnight delivery service to collect the donation immediately;
- Guarantees sweepstakes winnings in exchange for a contribution. By law, you never have to give a donation to be eligible to win a sweepstake; or

Tips to Avoid Charity Fraud:

- Visit **www.checkthecharity.com** to make sure a charity is properly registered with the Secretary of State, and visit the Better Business Bureau charity site at **www.give.org** to get information about a charity that has asked you for a donation.

- Ask for the solicitor's registration number and the registration number of the charity he or she is representing. If the solicitation is in person, ask to see identification for both the solicitor and the charity.
- Ask the solicitor how much of the donation will go to the charity. Reputable charities will gladly provide the information requested.
- Do not pay in cash. Donate with a check made payable directly to the charity.
- Watch out for charities with names that sound similar to well-known organizations. Sometimes these "sound-alike" names are simply intended to confuse donors.
- Beware of unsolicited e-mail. There have been numerous reports of e-mail that purport to be solicitations from well-known charities, such as the Red Cross or the United Way. These e-mails may also have links embedded in them that will take you to a fake charity website designed to steal your information.
- Do not respond to any e-mail soliciting donations for any organization. Instead, go directly to the organization's website.
- Further, such unsolicited e-mail may spread computer viruses. Do not respond to any e-mail soliciting donations from any organization. Instead, go directly to the organization's website or call the charity to make donations.
- Ask your tax advisor or the IRS if your donation will be tax deductible. The fact that a charity has a tax identification number does not necessarily mean your contribution is tax-deductible.
- Seniors can contact AARP ElderWatch via the Colorado Consumer Hotline by calling 1-800-222-4444, for more information on charity fraud.

Tips for Online Donating:

With more and easier access to the Internet, the advent of social media, the explosion of crowd funding Internet sites, and the ability to easily donate to a cause by simply clicking a button or sending a basic text message, it has become even easier than ever to donate to charitable organizations and specific causes.

- If you receive an e-mail or text message asking for a donation, confirm that the request is from the charity, and not an imposter, by contacting the charity or visiting its website.
- Check out the charity before you give to learn more about it through reputable sites such as the **Colorado Secretary of State's Office**, **IRS Select Check**, the Better Business Bureau's **Wise Giving Alliance**, or **Charity Navigator**.
- Be cautious of "look-alike" websites. These fraudulent websites will often ask for personal financial information or may download harmful malware into your computer.
- Watch out for charities with names that sound similar to well-known organizations. Sometimes these sound-alike names are simply intended to confuse donors.
- Don't assume that charity recommendations on Facebook, blogs, or other social media have already been vetted. Research the charity yourself.
- Find out what percentage of your donation will go to the charity and whether you will be charged any fees for making a donation through the fundraising platform website.
- Find out what the website will do (if anything) with your personal information; be wary of websites that do not provide a privacy policy.
- Be cautious when considering giving to newly formed charities since they won't have a track record that you can take into consideration.
- Be extra vigilant when donating online in the wake of natural disasters or national tragedies. Some charities are formed shortly thereafter and may have the best of intentions; however, an existing charity is more likely to have the sound management and experience to quickly respond to these situations, and it will have a track record which you can review.

Colorado Gives Day is an annual statewide movement to celebrate and increase philanthropy in Colorado through online giving. Visit **https://www.coloradogives.org/CoGivesDay** for more information or to donate.

SAFE SHOPPING

Be a Smart Shopper

With so many advertisements, special deals, and promised savings during the holidays, it makes sense to do some homework before you head to the mall. Here are a few important tips to help make you a smart shopper:

- Even if you're not going to shop online, you can do a lot of price and product comparisons on a store's website before you head out the door. You can also look at product reviews online before heading to your local store.
- If you're going to use a layaway plan for your holiday purchases, make sure to understand all terms and conditions of a merchant's layaway policy, including any additional costs.
- Get all of the details before agreeing to purchase an extended warranty or service contract on any purchase–you might be able to do this online before you go to the store.

- Keep all receipts and request gift receipts to ease any necessary returns of merchandise.
- Before completing your purchase, understand the merchant's cancellation, return and/or replacement policies. Will you receive credit on your card or just "store credits."
- A lot of times, advertised "sale prices" are actually manufacturer rebates—make sure you fully understand how a particular rebate program works, how you must apply, any deadlines for applying, and how the rebate is made (cash, prepaid credit card, store credit, etc.) **AND**, take the time to actually apply for any rebates!

Be a Safe Shopper

Big crowds, lots of excitement, and sometimes fast, last-minute shopping can cause you to forget some basic tips for staying safe during the holiday shopping season. Added stress can cause you to drop your guard. So, whenever possible:

- Shop during daylight hours. If you must shop at night, go with a friend or family member.
- Avoid wearing expensive jewelry.
- Do not carry a purse or wallet, if possible.
- Even though you are rushed and thinking about a thousand things, stay alert to your surroundings.
- Avoid carrying large amounts of cash.
- Pay for purchases with a check or credit card when possible.
- Keep cash in your front pocket.
- Avoid overloading yourself with packages. It is important to have clear visibility and freedom of motion to avoid mishaps.
- Beware of strangers approaching you for any reason. At this time of year, con-artists may try various methods of distracting you with the intention of taking your money or belongings.
- When you have to leave packages in your car, lock them in the trunk so they are not visible to other people walking by.
- Save your receipts in case you need to return or exchange items.
- Don't hesitate to ask store or mall security if you need an escort out to your car after dark.

CYBER SHOPPING

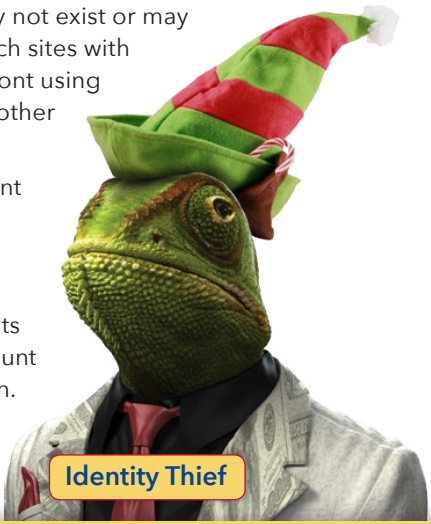
Tips for Online Shopping:

Shopping on the Internet can be fun, fast, and sometimes cheaper. Many retailers are only present on the Internet or provide special products and deals on their websites. Unfortunately, there are some hazards to online shopping that you should be careful to avoid. Here a few tips on staying "Cyber Safe" this holiday season:

- Make sure your computer and Internet browser security features are installed and contain the most current updates.
- Avoid unsolicited e-mails, text messages, and pop-up advertisements.
- Only shop on secured sites—look for websites that begin with "https" and/or display a small padlock in the bottom right corner of the site or in the address bar at the top.
- Don't use the same password on every shopping website—and the passwords you do use should not be simple numbers in sequences, birthdays, pet names, etc.
- Shop with online merchants you are familiar with or whose reputation you can readily determine.
- At a minimum, do some basic research to find out if the business is licensed and verify the company history with the Better Business Bureau.
- Confirm a working customer service number you can contact if you have further questions or product issues.
- Be suspicious of websites offering consumer goods at unbelievably low prices, especially on popular items such as brand name electronics. These sites may be trying to collect your personal information or actually be selling knock-off or counterfeit products, or real products that have been damaged, returned, and refurbished. Best advice—if a deal just sounds too good to be true, it probably is.
- Be wary of "free" gift card offers, especially through Facebook and other social media sites. You usually have to sign up with participating merchants and that means providing valuable personal and financial information to unscrupulous vendors.

- Make your online purchases with a credit card—federal law limits your exposure to $50 if your credit card is used improperly. Plus, you can charge back any purchases you think were fraudulent. Avoid companies that require less conventional forms of payment, such as money orders, electronic funds transfers, money transmitters (Western Union/MoneyGram), or the purchase of prepaid payment devices.
- Do not, under any circumstances, provide your checking account number.
- Before you finalize an online purchase, understand the merchant's cancellation, return and/or replacement policies. Find out whether you will receive credit on your card or just "store credits."
- Check the promised delivery date. The Mail, Internet, or Telephone Order Merchandise Rule (16 CFR Part 435) requires that a merchant advertising over the phone, mail or Internet must have a reasonable basis for stating or implying that they will ship purchased items within a certain specified time. If they make no statement about delivery time, they must have a reasonable basis for believing that they will ship within 30 days. The Rule also requires that, when a seller cannot ship within the promised time, the seller must obtain the buyer's consent to a delay in shipping or refund payment for the unshipped merchandise.

- Before you finalize an online purchase, understand the total amount you will be asked to pay, including shipping and handling charges, express delivery charges, and any restocking or similar fees if you have to return an item.
- Find and read the merchant's privacy policy to understand what information they are collecting about their customers, what they are doing with that information, and whether you are able to opt-out of having your information collected or shared.
- Don't provide more information about yourself than is necessary–there is no reason an online merchant should need your date of birth or social security number.
- Be wary of e-mail or text messages claiming to be from a courier service about a package that you don't know about–that message may direct you to a site to claim the package only to steal your personal or financial information.
- If you shop online using a mobile device, rely only on apps provided by a familiar and reputable online merchant–mobile device apps sent to you via unsolicited e-mail or text messages, or through pop-up ads, may contain malware or other viruses that can infect your mobile device.
- Be careful when using a public WiFi network to transact any business over the Internet. Even if the WiFi network is secure and password protected, you never know who might be sneaking a glance over your shoulder.
- Be wary of advertisements claiming to sell popular and hard to find items on auction sites such as eBay or on Internet classified sites such as Craig's List–the items may not exist or may be damaged. Don't do business on such sites with individuals that demand payment upfront using money orders, money transmitters, or other unconventional means.
- Keep a record of your purchase and print out a copy of your order form and any other correspondence you receive.
- Even if you follow all of these tips, you should check your credit card statements frequently to rapidly detect if your account is being used without your authorization.



THOSE QR CODES

You know those funny little, two-dimensional bar codes that seem to be in every advertisement and on every product? These are called "QR Codes"—which stands for Quick Response Codes. Different from traditional bar codes, QR codes can carry significantly more information. With the proliferation of QR code scanning apps on smart phones and other mobile devices, consumers can look up products, comparison shop at other online stores, and get immediate access to a variety of information. That is all well and good, but with any technological advances come predators that use the same technology to commit fraud.

Fake QR Codes can direct you to malicious websites where malware can be automatically downloaded into your mobile device or where your personal information and passwords can be compromised.

Here are a few tips for avoiding QR Code fraud:

- Make sure your smart phone or other device has updated anti-virus and malware protection installed and operating.
- Ensure that any QR code scanning app that you download is from a reputable source.
- Only use a QR code scanner app that has built-in security features, including the ability to inspect the decoded text prior to opening up the code in a browser or other targeted application.
- Never scan a random code box that has just been stuck on a wall, window, light pole, or even the ground.
- Even if there is other information, for instance when it's on a poster, be wary about scanning a code in public places, like transportation depots, bus stops or city centers.
- If you decide to scan, check first to see if the code is on a sticker that may have been pasted over the legitimate code.
- Never enter personal or financial information on a website to which you have been directed from a QR code.

NEED A LOAN FOR THE HOLIDAYS?

There may be a lot of financial pressure around the holidays—for gifts, travel, etc. You also may see a lot of holiday "special" offers on low interest rates, delayed payment or "zero interest" offers. If you absolutely must look for some consumer financing during this period (or anytime, really) here are a few things to consider:

- If you do feel the need to borrow, try to only borrow what you can afford to pay back. In order to avoid over-borrowing and curb impulsive spending, complete a budget analysis before the holiday shopping season begins. Keep a copy of your budget with you as a reminder to stick to your plan.
- If you feel you need to obtain a loan, first attempt to do so from a conventional source such as your bank. If you need to search further, apply for credit from a UCCC licensed lender who is regulated for compliance with lending laws—a list of licensed lenders can be found on our website at **www.coloradoattorneygeneral.gov/uccc**.
- Beware of online loans. Colorado law requires consumer lenders, including those offering loans online, to be licensed and limits the finance charges and other fees that they can charge you. Unfortunately, there are too many instances of online lenders ignoring Colorado law and charging consumers interest rates FAR in excess of what is allowed under Colorado law.
- Before you provide sensitive information to any creditor (such as banking info, SS#, etc.) ensure your information will be safeguarded. Inquire about the creditor's privacy policy—will your info be shared unknowingly with third parties?
- Limit your credit sources. Do not over-apply for credit through numerous sources. When applying for credit, creditors will obtain a credit report. Multiple creditors obtaining credit reports in a short period of time can negatively impact your credit score.

- Be careful with "free" financing offers. Many stores will offer zero interest financing for a small period of time (typically 3 to 6 months). Under this plan interest will not be charged if, and only if, you pay back the entire debt within the promotional period. However, if there is any balance at the time the promotional period ends, the creditor will then add the entire amount of interest that normally would have accrued during the promotional period.
- Considering layaway? Layaway deals have made a huge comeback in recent years and can be an option if you are trying to avoid debt. Not all layaway options are created equal. Look out for hidden fees by reading the fine print—how much and in what form do you get your money back if you decide to cancel? Are there restocking fees? What happens if the item goes on sale while on layaway?

WHAT DO YOU DO IF THERE ARE PROBLEMS?

For most of you, the holiday shopping season will be just what it is supposed to be: fun, family, food, and friends. For some, however, even following all of the tips in this Holiday Guide will not protect you from truly unscrupulous practices or outright fraud. You may have paid for goods that were never delivered or were not as advertised. Here are a few things you can do if you find yourself in that situation:

- Work directly with the merchant–in a professional manner–to see if any problems can be worked out informally.
- If you suspect that you are the victim of a fraud or scam you should contact your Better Business Bureau to file a report AND you should file a complaint with my office. You can call 1-800-222-4444 or file a complaint online at **www.stopfraudcolorado.gov**.
- If you suspect that you are the victim of a crime, contact your local law enforcement agency (police/sheriff's office) and file a complaint.
- If you suspect that you are the victim of identity theft, you should also contact your local law enforcement agency and you should visit my ID Theft Center at **www.stopfraudcolorado.gov/fraud-center/identity-theft** for more information.

If you believe you have been defrauded, your identity stolen or you've been the target of a scam, please visit **StopFraudColorado.Gov** and file a report. It is also important to quickly report crimes to law enforcement.

We at the Colorado Department of Law hope this *Consumer Holiday Guide* was helpful and we hope that you will share it with your friends and neighbors.

From the our team we wish you and yours a Merry Christmas, Happy Hanukkah and a prosperous New Year!

Colorado Attorney General
Cynthia H. Coffman

If you have been victimized by fraud or would like more information on how to report fraudulent activity, call the Colorado Consumer Hotline at:

Toll Free:	1-800-222-4444
Greater Denver Area:	303-222-4444
Outside of Colorado:	720-508-6006

REPORT FRAUD

Complaints may be filed through our website at:
www.stopfraudcolorado.gov/report

Register to receive future electronic fraud advisories and the *Consumer Fraud Awareness Bulletin* at **www.stopfraudcolorado.gov/fraudawareness**.

stopfraudco stopfraudco YouTube stopfraudco

Colorado Attorney General
Cynthia H. Coffman

November 2016