

# Consumer Fraud Awareness

Brought to you by Colorado Attorney General, John Suthers

## Department of Law

1525 Sherman Street  
Denver, CO 80203  
Phone: 303-866-4500  
Consumer Hotline: 800-222-4444  
[www.coloradoattorneygeneral.gov](http://www.coloradoattorneygeneral.gov)  
[Join us on Facebook](#)

## Highlights

- \* Online Dating Scams
- \* Phishing + Identity Theft
- \* Business Opportunities
- \* Consumer Resources

## Inside this issue:

Fraudulent Phone Calls	1
Payday Lending Scams	2
Online Dating Scams	2
Business Opportunities	3
Phishing+ Identity Theft	4
Internal Revenue Scams	4
Consumer Resources	5

As we begin 2012, Colorado consumers continue to be barraged with scams attempting to defraud consumers of their hard-earned income. Scammers will utilize a myriad of techniques to catch consumers off-guard as they pursue consumers personal information, which can ruin an individual’s financial future. Stolen identities, fraudulent billing issues, damaged credit ratings, and receipt of inoperable products are among the long-term effects of these scams. In severe cases, consumers may be faced with enormous financial hardships, including bankruptcy, loss of one’s home and/or other assets.

The Colorado Attorney General’s Office in partnership with state, federal, and private partners are dedicated to providing information and resources for consumers to utilize in identification of fraudulent activity. With the information contained in this newsletter, along with the numerous other resources available, we hope consumers continue to take the initiative to protect themselves and report these unscrupulous behaviors.

## Fraud Calls-Lower Interest Rates/Grandparent Scam

Consumers continue to receive unwanted telephone calls offering a variety of different products and services. Many of these offers are specifically designed to fraudulently capture your personal and financial information.

The most prevalent of these “robo calls” consist of pre-recorded messages from Account Services, Cardholder Services, or Card Services, supposedly offering a lower credit card interest rate.

The “robo calls” usually offer the consumer an option to speak with an agent or to have their telephone number removed from the telemarketer’s calling list by pressing a number. Pressing the number won’t stop the calls and may actually initiate additional calls.

If a consumer actually talks with someone and complains about the call or asks where the person is located, that person typically will just hang up. Any information provided by

the caller will most likely not be true. In no case should consumers sign up for these so-called interest rate, debt reduction services.

Among other active telephone scams, the “Grandparent Scam” claims a consumer’s grandchild is in legal trouble and locked up abroad in a foreign country.

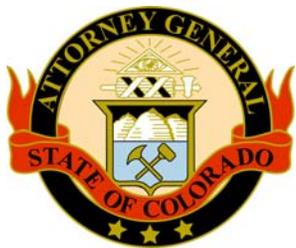
The caller will request the grandparent send money immediately and insist the grandparent not contact the grandchild’s actual parents.

These calls are phony. If you receive such a call, contact the parent to the whereabouts of the child immediately and never send money without taking extra steps to verify the legitimacy of the situation. In almost every case, this is fraud.

When receiving any type of fraudulent or unwanted call, hang-up the phone immediately and report the caller to both the [Colorado No-Call](#) and the [National Do-Not-Call Registry](#).



“As a native Coloradan and attorney with more than three decades of experience in the public and private sectors, I am dedicated to helping keep Colorado a great place to live.”



A Program with the Colorado Attorney General and the AARP Foundation

## Pay Day Lending and Loan Scams

Payday Loan and Collection Agency scams have increased dramatically in recent years. As a result, consumers are facing fraudulent telephone calls from scammers claiming the victim is delinquent on a payday loan or collection agency account and must repay the loan immediately to avoid immediate and direct legal action.

The caller represents themselves as being associated with various law enforcement and government agencies (Attorney General, FBI, Police Officials, Department of Homeland Security, etc.), as well as other seemingly legitimate law firms and collection agencies.

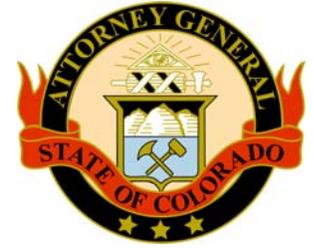
The callers have an overwhelming amount of personal information about the victim, including name, address, employer, social security number, bank account information, etc. The scammers get personal information from a variety of sources; however, many victims report receiving the scam calls shortly after completing loan and credit applications online.

The scammers constantly harass victims by calling their home, mobile, and work telephone numbers. They will threaten legal action, formal arrest, and in many cases will threaten physical violence in an effort to coerce the victim to pay. The callers typically request money to be paid immediately through Western Union,

Money Gram, a pre-paid credit card, or other means.

If you receive these calls:

- Never provide personal information over the phone or through email to an unknown source.
- Immediately contact local law enforcement if you feel threatened.
- If you have had a payday loan or collection account, verify the status of your account with your lender using information on your original loan documents.
- Get proof of the debt as debt collectors are required under Colorado law to provide proof on request.
- Verify the company is licensed to offer payday loans or collect debt within Colorado through the [Uniform Consumer Credit Code \(UCCC\)](#) and the [Collection Agency Board \(CAB\)](#) section of the Colorado Attorney General's Office.
- If contacted by telephone, file a complaint with the [Colorado No-Call](#) and the [Federal No-Call Registry](#). If contacted via email, file with the [Internet Crimes Center](#).




---

**Consumers are facing an enumerable amount of fraudulent telephone calls from scammers claiming the victim is delinquent on a payday loan or collection agency account and must repay the loan immediately to avoid direct legal action.**

---

## AARP ElderWatch—Online Dating

Looking for love in all the wrong places? Many older adults are looking for love and friendship online, but should stay alert for online dating scams.

What is an online dating scam? An online dating scam is when a scammer, male or female, creates a false personal profile and makes contact with you via an online dating agency or chat room. The scammer says that they are seeking romance or a soul mate but are really out to steal not only your heart but your cash too.

How do I know it is a scam?

The scammer will ask for your money! This will not happen immediately - however, before long the scammer will ask for financial help for any number of reasons.

Almost always, they will ask you to send money using an untraceable source such as a wire transfer service. Some of the most common reasons they give for why they need your help may include:

- They want to meet you but don't have enough money to travel to see you.
- They are stranded abroad and don't have money for return travel or visa costs,

or someone stole their wallet.

What can you do to protect yourself? Only use a reputable online dating or chat service and follow the basic safety tips for online dating.

Be skeptical and ask yourself simple questions like, "why am I the only person who can help them, but I have just met them?" These scammers will claim you are their one and only love, but really you are their one and only target!

*Amy Nofziger - Program Manager -AARP ElderWatch*  
[www.aarpelderwatch.org](http://www.aarpelderwatch.org)

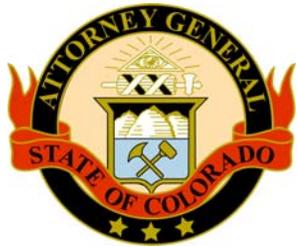
---

**To learn more about AARP-ElderWatch and their efforts to assist Colorado seniors, please visit:**  
[www.aarpelderwatch.org](http://www.aarpelderwatch.org)

---



**A Program with the Colorado Attorney General and the AARP Foundation**



**Unfortunately, too many people invest nearly all of their savings in opportunities that promise tremendous income with little effort, only to lose everything.**

Many consumers are drawn to seminars and infomercials which promise income generating business opportunities. While there are a number of legitimate and successful franchise opportunities available, most are very expensive and require a tremendous amount of energy and effort. In general, franchises and business opportunities are not regulated in Colorado.

Unfortunately, too many people invest nearly all of their savings in opportunities that promise tremendous income with little effort, only to lose everything.

The Federal Trade Commission has a Franchise and Business Opportunity Rule which they enforce (16 C.F.R Part 436). This rule requires franchise and business opportunity sellers to give you specific information about their business opportunity, at least 10 days before you pay any money or legally commit yourself to a purchase. That information includes:

- Names, addresses and telephone numbers of at least 10 previous purchasers who live closest to you;
- A fully audited financial statement of the seller;
- Background and experience of the business' key executives;
- Cost of starting and maintaining the business, and the responsibilities you and the seller will have to

each other once you've invested in the opportunity

If the seller doesn't give you a disclosure document, ask why. Verify the opportunity with an attorney, a business advisor or the FTC by calling its toll-free helpline at 1-877-FTC-HELP (382-4357). Even if the business is not legally required to provide a disclosure document, you still may want one for your own information.

Here are some important tips provided by the FTC:

- Study the disclosure document and proposed contract carefully.
- Interview current owners in person.
- Don't rely on a list of references selected by the company because it may contain false or misleading information.
- Ask owners and operators how the information in the disclosure document matches their experiences with the company.
- Investigate claims about your potential earnings. Be suspicious of any company that does not show you in writing how it computed its earnings claims.
- Sellers also must tell you in writing the number and percentage of owners who have done as well as they claim you will.
- Recognize that once you buy the business, you may be competing with franchise owners or inde-

pendent business people with more experience than you.

- Shop around. Compare franchises with other business opportunities. Some companies may offer benefits not available from the first company you considered.

The Franchise Opportunities Handbook, published annually by the U.S. Department of Commerce, describes more than 1,400 companies that offer franchises.

Consumers tips include the following:

- Contact only those opportunities that interest you, request their disclosure documents and compare their offerings.
- Listen carefully to the sales presentation. Some sales tactics should signal caution. For example: if you are pressured to sign immediately "because prices will go up tomorrow," or "another buyer wants this deal," slow down. Be wary if the salesperson makes the job sound too easy. The thought of "easy money" may be appealing, but success generally requires hard work.
- Get the seller's promises in writing and consider getting professional advice before you invest. Ask a lawyer, accountant or business advisor to read the disclosure document and proposed contract.

If you believe you have been deceived by a franchise or business opportunity, file a formal complaint with the [Federal Trade Commission](http://www.ftc.gov).



A Program with the  
Colorado Attorney General  
and the AARP Foundation

## Phishing and Identity Theft

Phishing has been around in various forms and used by scammers for decades in an attempt to gain personal and financial information for fraudulent purposes. With the advanced popularity of the Internet and email correspondence, Phishing has become a more efficient and effortless fraud to perpetrate. As a result, Phishing has gained even more popularity among scammers.

Dictionary.com defines the word Phish as: “to try to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake Web site that replicates the real one.”

According to the Federal Trade Commission (FTC), consumers should follow the following tips to avoid becoming victimized from phishing:

- If you get an email or pop-up message that asks for personal or financial information, do not reply. Legitimate companies don't ask for this information via email.

- If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine or type in the listed Web address yourself.
- Don't cut and paste the link from the message into your Internet browser—phishers can make links look like they go to one place, but that actually send you to a different, fraudulent site.
- In any case, delete random emails that ask you to confirm or divulge your financial information.
- A firewall helps make you invisible on the Internet and blocks all communication from unauthorized sources.

**Use anti-virus and anti-spyware software, as well as a firewall and update them all regularly.**

- Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge.
- Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files.
- Anti-virus software scans incoming communications for troublesome files.

**Review credit card and bank account statements as soon as you receive them.**

- Check for unauthorized charges.
- If your statement is late by more than a couple days, call your credit card company or bank to confirm your billing address and account balances.

**Be cautious about opening any attachment or downloading any files from emails.**

- These files can contain software that can weaken your computers security.

**Forward spam that is phishing for information to:**

- spam@uce.gov and to the company, bank, or the organization impersonated in the phishing.

If you believe you have been scammed from phishing, file a complaint with the [FTC](#) and review the [Colorado Attorney General's Identity Theft Handbook](#).

## Internal Revenue Service Scams

With the 2011 tax year quickly coming to an end, consumers should be aware and cautious of any email correspondence from the Internal Revenue Service.

Per the IRS, “the IRS does not initiate taxpayer contact via unsolicited email or ask for personal identifying or financial information via email. If you receive a suspicious email claiming to come from the IRS, take the following steps:

- Do not open any attachments or links contained within the email, as they may contain malicious code that will infect your computer.
- Do not click on any links for the same reason. Be aware that the links often connect to a phony IRS Web site that appears authentic and then prompts the victim for personal identifiers, bank or credit

card account numbers or PINs. The Web sites appear legitimate because the appearance and much of the content are directly copied from an actual page on the IRS Web site and then modified by the scammers for their own purposes.”

Concerned consumers should contact the IRS at 1-800-829-1040 immediately.

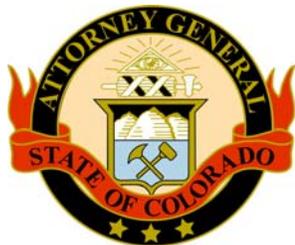


**Phishing has become a more efficient and effortless fraud to perpetrate. As a result, Phishing has gained even more popularity among scammers.**

**If you receive fraudulent IRS emails and other correspondence, forward the suspicious email or the url address to the IRS mailbox [phishing@irs.gov](mailto:phishing@irs.gov), then delete the email from your in-**



**A Program with the Colorado Attorney General and the AARP Foundation**



## Consumer Resources

### Colorado Attorney General

1525 Sherman Street  
Denver, CO 80203  
[www.coloradoattorneygeneral.gov](http://www.coloradoattorneygeneral.gov)

### Consumer Protection Line:

Toll Free: 800-222-4444  
Metro Denver: 303-222-4444  
[www.coloradoattorneygeneral.gov/cp](http://www.coloradoattorneygeneral.gov/cp)

### Collection Agency Issues

**Colorado Collection Agency Board**  
303-866-5304  
[www.coloradoattorneygeneral.gov/cp](http://www.coloradoattorneygeneral.gov/cp)

### Fraudulent or Unwanted Calls

**Colorado No-Call**  
Local: 303-776-2675  
Toll Free: 800-306-7041  
[www.coloradonocall.com](http://www.coloradonocall.com)

### Uniform Consumer Credit Code

303-866-4494  
[www.coloradoattorneygeneral.gov/cp](http://www.coloradoattorneygeneral.gov/cp)

### AARP ElderWatch

Toll Free: 800-222-4444  
Metro Denver: 303-222-4444  
[www.aarpelderwatch.org](http://www.aarpelderwatch.org)

### Better Business Bureau

[www.bbb.org](http://www.bbb.org)  
Denver/Boulder  
303-758-2100  
Northern Colorado  
970-484-1348  
Southern Colorado  
719-636-1155  
Western Colorado  
505-346-0110

### Citizens Advocate Office

127 State Capitol  
Denver, CO 80203  
Toll Free: 800-283-7215  
Main Office: 303-866-2885  
[www.colorado.gov](http://www.colorado.gov)

### Colorado Foreclosure Helpline

1-877-601-HOPE (4673)  
[www.coloradoforeclosurehotline.org](http://www.coloradoforeclosurehotline.org)

### Federal Bureau of Investigation

**(FBI) - 303-629-7171**  
8000 East 36th Ave  
Denver, CO 80238  
[www.fbi.gov](http://www.fbi.gov)

### Federal Trade Commission (FTC)

**Do-Not-Call Registry**  
[www.donotcall.gov](http://www.donotcall.gov)

### Federal Trade Commission (FTC)

Toll Free: 877-382-4357  
<http://www.ftc.gov/>

### Identity Theft

Colorado Bureau of Investigations (CBI):  
Identity Theft Hotline: 855-443-3489  
[www.cbi.state.co.us](http://www.cbi.state.co.us)

### Internet Crimes Center

[www.IC3.gov](http://www.IC3.gov)

### Legal Resources

Colorado Bar Association  
Toll Free: 800-332-6736 (in Colorado)  
Local: 303-860-1115  
[www.cobar.org](http://www.cobar.org)

Can't find what you're looking for? Please view the Colorado Attorney General Consumer Resource Guide for additional tools and resources at:

[www.coloradoattorneygeneral.gov](http://www.coloradoattorneygeneral.gov)



A Program with the  
Colorado Attorney General  
and the AARP Foundation

*Not on the registration list? Visit us on the Web to ensure receipt of future correspondence at:*  
[www.coloradoattorneygeneral.gov/fraudawareness](http://www.coloradoattorneygeneral.gov/fraudawareness)

Join us on Facebook