

# SCAMS

Protect Yourself. Protect Your Money.



17 North Second Street | Suite 1300  
Harrisburg, PA 17101

1.800.PA.BANKS (1.800.722.2657)  
dobs.pa.gov



Financial Services for Consumers and Business



Property of the Pennsylvania Department of Banking and Securities

version12.2016



FRAUD



protect. regulate. inform.

## Take action today:



Connect ... Learn ... Contact

**Connect:** PA Banking and Securities on Facebook and LinkedIn. @PAFinancialReg on Twitter. Stay connected to learn of events in your community, as well as the latest financial and regulatory news and trends.

**Learn:** [dobs.pa.gov](http://dobs.pa.gov) | [The Quarter](#)  
We have numerous **FREE** publications and resources for consumers and community organizations.

**Contact:** 1.800.PA.BANKS or (1.800.600.0007). Our phones are staffed from 8:00 AM to 5:00 PM Monday through Friday. A live person will answer your call or return your call within 24 hours during the week.

***"By failing to prepare,  
you are preparing to fail."***

-Benjamin Franklin

## Other Contacts

### National Federation for Credit Counseling

• 1-800-388-2227 • 1-800-682-9832 (Spanish)

[nfcc.org](http://nfcc.org)

### Financial Industry Regulatory Authority (FINRA)

BrokerCheck® (research Brokers, Brokerage Firms, Investment Adviser Representatives and Investment Adviser Firms)

[finra.org/Investors/ToolsCalculators/BrokerCheck/](http://finra.org/Investors/ToolsCalculators/BrokerCheck/)

### Area Agencies on Aging

[aging.pa.gov/local-resources/pages/AAA.aspx](http://aging.pa.gov/local-resources/pages/AAA.aspx)

## Free Credit Reports

**Annual Credit Report Request Service** • P.O. Box 105281, Atlanta, GA, 30348-5281

1-877-322-8228

[annualcreditreport.com](http://annualcreditreport.com)

## Credit Bureaus

**Equifax** • 1-800-685-1111

[equifax.com](http://equifax.com)

**Experian** • 1-888-397-3742

[experian.com](http://experian.com)

**TransUnion** • 1-888-567-8688

[transunion.com](http://transunion.com)

## Better Business Bureaus

**Western Pennsylvania** • 877-267-5222 (Pittsburgh)

[westernpennsylvania.bbb.org](http://westernpennsylvania.bbb.org)

**Northeastern Pennsylvania** • 570-342-5100 (Scranton)

[nepa.bbb.org](http://nepa.bbb.org)

**Eastern Pennsylvania** • 215-985-9313 (Philadelphia) • 610-966-8780 (Bethlehem)

• 717-364-3250 (Harrisburg)

[easternpa.bbb.org](http://easternpa.bbb.org)

# Who to Contact for Help

## Government Agencies



### **Pennsylvania Department of Banking and Securities**

Trying to find information on financial services can be confusing, so if you are not sure where to start, call us today at **1.800.PA.BANKS** or **1.800.600.0007**.  
[dobs.pa.gov](http://dobs.pa.gov)

### **Pennsylvania Office of Attorney General**

• 1-800-441-2555  
[attorneygeneral.gov](http://attorneygeneral.gov)

### **Pennsylvania Department of State, Bureau of Charitable Organizations**

• 1-800-732-0999  
[dos.pa.gov](http://dos.pa.gov)

### **Federal Trade Commission**

• 1-877-FTC-HELP  
[ftc.gov](http://ftc.gov)

### **Consumer Financial Protection Bureau**

• 1-855-411-2372  
[consumerfinance.gov](http://consumerfinance.gov)  
[consumerfinance.gov/es](http://consumerfinance.gov/es) (Spanish-language website)

### **Internet Crime Complaint Center • [www.ic3.gov](http://www.ic3.gov)**

### **U.S. Secret Service**

• Harrisburg 717-234-0214 • Philadelphia 215-861-3300  
• Pittsburgh 412-281-7825 • Scranton 570-346-5781  
[secretsservice.gov](http://secretsservice.gov)

### **Internal Revenue Service**

(For information about charitable organizations)  
• 1-877-829-5500  
[irs.gov/charities](http://irs.gov/charities)

# Protect Yourself. Protect Your Money.

Every day, thousands of people are taken advantage of by professional criminals and con artists using slick and sophisticated methods to steal people's money. Often, even as the crime is being committed, the victim is unaware of the scam. Too often, the victims feel ashamed because they placed their trust in people who stole from them – and they are too embarrassed to report the crime. If you have fallen victim to a financial scam, you are not alone.

One of the best ways to protect yourself from financial scams is to be informed. The Pennsylvania Department of Banking and Securities has created this brochure to include information about some of today's most common scams, as well as helpful tips to protect yourself and your money. You can also find information on how to contact government agencies, nonprofit organizations and credit bureaus who can help you protect yourself or help you if you have fallen victim to a scam.

**Keep in mind that, with every opportunity, if it sounds too good to be true, it probably is!**

## Contents

Pay Up Front Scam	2
Affinity Fraud	3
Charity Scams	4
Counterfeit Cashier's Check Scam	5
Credit Repair Scams	6
The Romance Scam	7
The "Microsoft Scam"	8
International Lotteries	9
The IRS Scam	10
Ponzi Schemes	11
Who to Contact for Help	12-13

Pay Up Front Scam



Advance fees, or upfront payments, are an instant “red flag.” Advance fee con artists pose as representatives of companies that seem real. They use slick presentations to trick their victims into paying large upfront fees for bogus loans, loan modifications, loan refinancing or credit cards. They frequently target individuals with poor credit histories by promising easy or “guaranteed” approval. However, in order to take advantage of the offer, the victim must pay high but seemingly legitimate fees for the application, insurance or other “services.” In the end, the scam artist takes off with the fee and the victim gets nothing in return.

People encounter advance fee scams in a variety of ways, including telemarketing calls, text messages, emails, well-designed documents, classified ads and the Internet, including social media.



Protect Yourself

- Avoid any credit offer that requires an upfront payment. Although a lender may charge application, credit report and other fees, they are generally subtracted from the loan amount after it is approved.
- If you are asked to pay fees via a wire transfer or prepaid debit card, especially to someone in another country, exercise caution. Such payments are extremely difficult to recover or trace.
- Know who you are dealing with. If you have not heard of the person or company, take the time to learn more about them.
- If you become a victim of an advance fee scam, contact the Pennsylvania Department of Banking and Securities, the Pennsylvania Office of Attorney General or the Federal Trade Commission.

2

► See Pages 12-13 for contact information of organizations that can assist you.

Ponzi schemes are named after the early 20th century swindler Charles Ponzi, whose most infamous modern successor is Bernie Madoff. Ponzi schemes take many forms, but they all depend upon a steady stream of investors who are promised regular, abnormally high rates of return. Without a steady stream of new investors, the Ponzi scheme becomes a “house of cards” that collapses under its own weight, with the scam artist long gone with investors’ money.



Ponzi schemes can be difficult to spot, but here are some of the “red flags”:

- ▀ Victims are urged to cash in on a quick, speculative scheme.
- ▀ Investors are promised that their investment is “risk free.”
- ▀ Ponzi promoters often depend on social circles: early investors unwittingly line up their closest friends, relatives and professional associates as new victims.
- ▀ Early investors are paid off handsomely. This is the “proof” that later, more skeptical investors insist on seeing before they jump in with both feet.



Protect Yourself

- All legitimate investments involve a degree of risk. Beware of promises of high, guaranteed, “risk free” profits.
- Avoid promoters who refuse to provide clear and detailed explanations of their investment vehicles.
- Don’t be rushed into making a decision. Beware of sellers creating a false sense of urgency to immediately invest.
- Check out the promoter’s background through FINRA’s Broker Check (Page 13).
- Make sure the investment is registered as a securities offering with the Pennsylvania Department of Banking and Securities or the federal Securities and Exchange Commission.
- Ask for detailed information in writing and verify the promoter’s claims.
- Be cautious of deals that cannot be checked out in person.
- Look for un-businesslike conduct or disruption of promised services.
- If you become a victim, contact the Pennsylvania Office of Attorney General, the Pennsylvania Department of Banking and Securities or your local law enforcement agency.

11

► See Pages 12-13 for contact information of organizations that can assist you.

## The IRS Scam



You have received a phone call or email from someone claiming to be working for a government agency like the Internal Revenue Service or the U.S. Treasury. Even though you have not received any notices from the government, the caller claims that you owe money for unpaid or back taxes, or that you missed a paperwork deadline.

The caller then threatens you with arrest or lawsuit if you do not pay them or give them personal information (for example, your Social Security number or date of birth). The caller demands that you wire them money, purchase a prepaid debit card, or otherwise arrange to send them money in ways that cannot be traced.

The caller sounds demanding and authoritative. What are you supposed to do?



### Protect Yourself

- Remember: no U.S. government or state agency is going to call you out of the blue and demand money or information
- While they may contact you via phone, the U.S. government and state agencies will always send important legal information by mail
- If you do not recognize a telephone number on caller ID, you do not have to answer the phone (even if caller ID says it is the IRS or some other government agency)
- Legitimate callers will leave you a message
- If you think it may be legitimate, take the caller's name and hang up. Don't call the number the caller provided, rather look the up telephone number in a directory and be sure that you are calling the actual agency and not a scam artist
- If you are a victim, contact the Pennsylvania Office of Attorney General.

# 10

► See Pages 12-13 for contact information of organizations that can assist you.

## Affinity Fraud

Affinity fraud takes place when a con artist claims to be a member of the same ethnic, religious, career or community-based group. "You can trust me," says the con artist, "because I'm like you. We share the same background and interests. And I can help you make money."

These scam artists frequently pay high returns to early investors in the group with money generated from later investors. As a result, early investors might be wildly enthusiastic about a scheme that collapses once you have invested, with the victim's money long gone with the scam artist.

Religious affinity fraud remains a widespread problem, with swindlers found across all denominations. Consumers have complained about fraud and abuse by financial planners, con artists claiming church endorsements, and givers of "divinely inspired" investment advice.

Many of the scams are based on dire predictions of imminent financial and social chaos, such as a sharp drop in the stock market. Specialized media outlets, religious-oriented magazines, newspapers, radio stations and cable television outlets make it easy for con artists to target the faithful.



### Protect Yourself

- Be cautious about the use of names or testimonials from other group members.
- Don't be rushed into making a decision. Beware of sellers creating a false sense of urgency to immediately invest.
- Obtain a prospectus or other form of written information that details the risks in the investment, as well as procedures for getting your money out.
- Ask for professional advice from a neutral outside expert not in your group - an accountant, attorney or Certified Financial Planner - to evaluate the investment.
- Investigate before you invest: Call the Pennsylvania Department of Banking and Securities to ensure that the investment is legally registered or use FINRA's Broker Check (Page 13) to learn about the promoter's background.
- If you become a victim of affinity fraud, contact the Pennsylvania Office of Attorney General, the Pennsylvania Department of Banking and Securities or your local law enforcement agency.



# 3

► See Pages 12-13 for contact information of organizations that can assist you.



There are many organizations that do good work for worthy causes and deserve support. Unfortunately, there are people who view the generosity of others as an opportunity to line their own pockets.

Charity scams occur all the time, but are especially common after a major disaster or tragedy, such as Boston Marathon terrorist attacks or Hurricane Sandy, when the public is eager to give.

Fake charities often use names similar to those of well-known organizations. Victims may be contacted by email (something real charities only do with their existing stakeholders), by phone or by a "volunteer" going door-to-door. Charity scams can also be vehicles for identity theft by directing victims to

bogus websites where they provide personal and financial information along with their "donation."



### Protect Yourself

- Ignore email solicitations for donations from unknown organizations: they are almost always scams.
- Check with the Internal Revenue Service to make sure the organization asking you for money is registered as a 501(c) corporation. That means your donation is tax deductible.
- NEVER give cash. When writing a check, make it payable to the organization, not an individual or "cash."
- If a charity claims to be helping a local organization such as a police or fire department, check with that organization to see if they are indeed fundraising and using that charity.
- Contact the Pennsylvania Department of State to verify that the charity asking you for money is legally registered.
- You can also check the Better Business Bureau's Wise Giving Alliance for information on charities.
- If you are a victim, file a complaint with the Federal Trade Commission, the Internet Crime Complaint Center or, if appropriate, your local police department.

► See Pages 12-13 for contact information of organizations that can assist you.



Someone you do not know has just informed you that you have hit the jackpot in a foreign lottery or sweepstakes. You do not recall entering, but the prize is in your name. Unfortunately, this apparent stroke of good luck is usually just another scam.

Lottery scams work by persuading the victim to send money in order to claim a prize such as cash, a trip, or other item of value. The scam artist, who may claim to be representing a foreign government, celebrity or lottery organization, tells the victim the money is needed to cover insurance, security or other "processing fees" associated with disbursing the prize. Bank account or Social Security numbers may also be requested in order to "verify" the winner's identity. However, the prize never comes and the scam artist makes off with the victim's money and, perhaps, identity as well.

Other times, the intended victim will receive an unsolicited check or money order with directions to deposit the money and wire a portion of it back to the sender to cover "processing fees" or taxes. The check is fake; however, the money the victim has wired to the scammer is real. The victim cannot recover the funds sent by wire transfer and will be liable to their bank or credit union for any money they drew against the fake check.



### Protect Yourself

- Never give your bank account number to somebody so they can forward lottery winnings or other unexpected income to you. Scammers may use your bank account number to take money out of your account rather than to put money in it.
- Be suspicious of anyone who claims you have won something, especially if you do not remember entering a contest.
- It is against federal law to buy foreign lottery tickets by phone or mail.
- Legitimate lotteries and sweepstakes do not require winners to pay money before claiming a prize.
- If you are a victim, file a complaint with the Internet Crime Complaint Center.

► See Pages 12-13 for contact information of organizations that can assist you.

## The "Microsoft Scam"



You have received an unexpected phone call or an email from someone claiming to work for Microsoft or some other computer software company. This person claims that they have identified your computer as being infected with a virus, and offers to fix the problem.

In order to perform the "fix," you will be asked to pay a fee by providing your credit or debit card information (this could be \$50 or more). This person – a scam artist -- will ask for access to your computer's systems and software from wherever they are located.

While performing the so-called fix, you will see movement of the cursor on your computer screen, controlled by the scammer. This person may even pop open a window on your screen showing all the viruses and malware supposedly discovered during the "fix."

What is actually happening is that software, malware, and even viruses are being downloaded to your computer. Your system, files, and information have been compromised.

You may not discover that your computer has been taken over by a scam artist for days, weeks, or even months – and during this time, the scammer has been watching your every move on your own computer. The scam artist may even have downloaded "ransomware" onto your computer – you will not be able to access your computer files until you pay a ransom to the scammer. And once you've paid, you still may not get back access to your computer files.



### Protect Yourself

- Make sure you have current, effective anti-virus software installed on your computer
- If a person calls claiming to work for specific company, like Microsoft or Norton, tell them you will call them back. Call that company using a phone number you have verified as legitimate (from the telephone book, or actual company website).
- If you have received an email, contact the company's customer support website and ask the company to verify that this person is actually one of their employees.
- If you believe your computer is infected, avoid using the Internet and:
  1. Run a scan using your anti-virus software; or
  2. Contact a reputable computer repair technician or company and have them check your computer.
- If you are a victim, contact the Pennsylvania Office of Attorney General.

▶ See Pages 12-13 for contact information of organizations that can assist you.

## Counterfeit Cashier's Check Scam



There was a time when cashier's checks were considered the next best thing to cash. Today, sophisticated forgeries of this once trusted payment method are being used to bilk private sellers out of big cash.

This scam targets individuals selling expensive items such as cars, apartments, or even horses, through classified advertising and online auctions. The counterfeiter, who is often in another country, poses as an interested buyer and offers to pay with a cashier's check. After the victim presents the check to the bank, the buyer suddenly backs out of the deal and asks for a refund. Because the funds from the check are available from the bank after a few days, the victim assumes the check has cleared and agrees to return the money. By the time the bank discovers the forgery, up to 60 days later, the bogus buyer is long gone and the victim must now repay the bank for the amount of the fake check.

In other cases, the counterfeiter may send a cashier's check for more than the asking price of the item and then ask the victim to wire the "overpayment" back or to a third party.



### Protect Yourself

- Understand that although the bank may allow you to withdraw money soon after depositing a cashier's check, that does not mean the check has cleared.
- Remember: You are responsible for the funds you deposit until your bank has received the money from the institution where the check originated or the true account holder of the originating check reports the fraud (this could take more than 60 days).
- Be cautious of transactions with strangers who pay with cashier's checks. Make sure to tell the buyer that you will send the item only after the check has cleared. If you do not know the person presenting the check, hold the funds in your bank account until your bank confirms that the check has cleared.
- Avoid any situation where someone overpays for an item and demands that the extra money be returned.
- If you are a victim, contact the Pennsylvania Office of Attorney General, the U.S. Secret Service or the Pennsylvania Department of Banking and Securities.

▶ See Pages 12-13 for contact information of organizations that can assist you.

8

5

## Credit Repair Scams



Lots of companies claim they can “erase” or “repair” your credit history – for an upfront fee. But the truth is that only time and paying down your debts can improve your credit rating.

Dishonest credit repair companies may charge hundreds, even thousands of dollars for services they never perform. Others bill customers for things they can do on their own for free, such as disputing errors and removing outdated items.

In one common credit repair scam, the credit repair company disputes all the negative information in an individual’s credit reports. This usually results in some of the information being removed temporarily by the credit bureaus while the disputes are reviewed. During this time, the individual’s credit appears to have improved.

However, this is neither a legitimate or permanent fix.

Another trick is advising an individual to apply for a new Employee Identification Number (EIN) from the Internal Revenue Service and then use that number, which has the same number of digits as a social security number, to apply for credit. This is known as “file segregation” and it is a felony.



### Protect Yourself

- No one can erase negative information from your credit reports if it is accurate.
- You can correct mistakes on your credit report yourself.
- You are entitled to a free copy of your credit report from each of the three credit bureaus once every 12 months.
- You can contact the National Foundation for Credit Counseling to find an accredited credit counselor near you.
- If you are a victim, contact the Federal Trade Commission.

# 6

► See Pages 12-13 for contact information of organizations that can assist you.

## The Romance Scam



You have met someone in another city, state, or country online through an online dating profile or social media. **WARNING!** This person may be “catfishing” you – a person on the Internet not being who they claim to be.

This person makes him or herself attractive to you, and begins texting, emailing, or even calling you regularly. He or she claims to have fallen in love with you quickly, thereby forming a swift emotional attachment.

Next thing you know, this new love interest has experienced some type of crisis and needs your help quickly. Or maybe you have made plans to marry, which will require travel, a visa, or other wedding-related expenses.

This person needs money and asks for your help – through a money transmitter like Western Union, Money Gram, or by loading up a prepaid debit card. Or you may be asked to provide access to your bank account to make money transfers more easily.

He or she will stay in touch with you and promise anything as long as you keep sending money. You will never actually meet this person and you will not be able to trace the money you sent.



### Protect Yourself

- Avoid giving too many personal details about yourself until you are confident that you have come to know the person who is interested in you.
- Do not accept everything he or she tells you at face value.
- Google your “new love” and pay attention if his or her photo shows up with multiple names attached to it.
- If the person’s profile disappears from your dating website within a few days, there’s a good chance it was a fraud.
- Ignore out of the blue requests from potential spouses who are just looking for a free ticket.
- If you are a victim, contact the Pennsylvania Office of Attorney General.

# 7

► See Pages 12-13 for contact information of organizations that can assist you.