REPORT A SCAM/ID THEFT

Kentucky Office of the Attorney General ag.ky.gov/scams (502) 696-5300

Please complete this form to report a scam or ID Theft. Your report provides the Office of the Attorney General the information needed to spot scam/ID Theft trends in Kentucky. It also allows us to develop our consumer outreach programs based on the most current reports from our citizens. To assist you in completing this form, a reference sheet of some of the most common scams is included.

CONSUMER

Your Name: _____

Address: _____

City: _____ **State:** _____ **Zip Code:** _____

Phone number : _____ **Veteran: Yes** ☐ **No** ☐

Email address: _____

Are you 60 years of age or older? **Yes** ☐ **No** ☐ **(Optional)**

How Contacted

By phone: ☐ Phone Number of caller: _____

Was it an automated call? Yes ☐ No ☐

Were you provided another number to call back? Yes ☐ No ☐

If so, please provide the phone number: _____

By internet: ☐ Website: _____

Email address: _____

By mail: ☐ Name/Address of sender: _____

Type of Scam

☐ **Jury Duty Scam**– caller pretends to be law enforcement threating arrest for missed jury duty.

☐ **IRS/Treasury Scam**– caller uses threat of arrest for back taxes owed.

☐ **Grandparent Scam**– caller claims to be a grandchild in trouble and asks for money.

☐ **Government Grant Scam**– claims that you qualified for free money through the government.

☐ **Pay Day Loan Lender Scam**– claims you have an unpaid debt and uses threats of arrest .

☐ **Computer Scam**—Microsoft Impersonator warns of computer virus or locks computer for "ransom" money.

☐ **Sweepstakes/Lottery Scam**-claims that you won money or prizes but you must pay first.

☐ **Fake Employment Scam**– you receive a check with instructions to cash it and wire money.

☐ **Fake Check Scam**– scammer responds to your sales ad and sends larger check than asked for. **Card Member Services Scam**- caller offers lower interest rates on credit cards.

☐ Other, please explain: _____

_____

Did you lose money? Yes ☐ No ☐ If so, how much? $ _____

How did you send the money? _____

* **If you lost money, immediately contact the money service provider (such as Western Union, MoneyGram, i-Tunes, Green Dot, your credit card company, or financial institution) to report that the transaction was a scam and ask if the transaction can be canceled.**

Type of ID Theft

ID Theft occurs when your personal information is compromised and used to file taxes in your name or obtain credit, loans, utility service, government benefits, etc. in your name. Please visit IdentityTheft.gov to obtain information on steps to protect yourself or visit www.ag.ky.gov for an Identity Theft Victims Kit.

Were you contacted by a company or agency regarding a data breach? Yes ☐ NO ☐

If Yes, who contacted you? : _____

Was your identity used to open new accounts, etc.? ☐ Yes ☐ NO

Other, please explain? _____

_____

Please briefly describe your situation involving the scam or potential identity theft . You may also attach any **copies** of documents you received or **copies** of receipts you may have.

_____

_____

_____

_____

_____

_____

_____

_____

_____

Signature _____ Date _____

Please return form to:

Kentucky Office of the Attorney General

ATTN: Office of Senior Protection Scam/ID Theft

1024 Capital Center Drive, Suite 200

Frankfort, KY 40601

This complaint will be an open record subject to the applicable exemptions pursuant to KRS.61.878. The Office Of the Attorney General does not Discriminate on basis of race, color, national origin, sex, religion, age or disability in employment or the provision of services, and provides, upon request, reasonable accommodations.

Reference Information for Many Current Scams

Jury Duty Scam: The caller claims to be law enforcement informing you of an outstanding warrant for your arrest because you failed to appear for jury duty. The caller tells you to purchase pre-paid cards to pay for the fees associated with the warrant. Once you provide the numbers on the card, the caller can deplete the money from the cards and it is near impossible to trace. If you have concerns about any warrants, contact your local officials directly.

IRS/Treasury Scam: Also known as the IRS Impersonation scam. The caller claims to be an IRS official and informs you that you owe back taxes from previous years and uses threats of arrest if not paid immediately. The IRS will **never** contact you by phone or email concerning such matters. These calls should be reported to **the Treasury Inspector General for Tax Administration (TIGTA) at www.treasury.gov/tigta or call TIGTA at 800-366-4484.** If you think you owe back taxes or have any questions about this, contact the IRS directly at 800-829-1040.

Grandparent Scam: The caller pretends to be your grandchild who needs your help and requests money immediately. The "grandchild" pleads with the grandparent not to tell anyone. Wiring services, pre-paid credit cards and i-Tunes cards are often used in this scam. If you receive a similar call, hang up and contact the child's parents or call the child directly on his/her cell phone to inquire of his/her whereabouts.

Government Grant Scam: This caller or online gimmick claims that you qualify for a government grant because you "have never been arrested", or "you are a good citizen" or "you pay your taxes on time", etc. You may be asked questions about your financial needs. To receive the "grant," you must submit a fee. **Do not send any money or purchase pre-paid cards**. Do not provide any personal information to these callers.

Pay Day Loan Lender: The caller claims you owe an unpaid debt and uses threats of arrest if you do not pay immediately by pre-paid cards or gift cards. Note: they may even have a portion of your social security number. Please be aware that online payday lenders are illegal in KY! Furthermore, legitimate debt collectors are required to provide you with a written statement of the debt, per the Fair Debt Collection Practices Act. If you do not receive this, you should assume that it is a scam.

Computer Scam: The caller claims to be from Microsoft/Windows and has detected a "virus" on your computer and requires remote access to "remove" it. Microsoft Corporation will not call consumers in this manner. Some computer hackers may be able to "lock" your computer and demand "ransom" money in order for you to access your computer again. Be wary of any unknown sites or opening messages from anyone unknown to you. You could unknowingly have malware installed on your computer.

Sweepstakes/Lottery Scam: These scams often come by mail or over the phone. Impersonators often use the Publisher's Clearing House name in order to appear legitimate. The caller then indicates that you have won an expensive prize, but you must first pay a fee. **It is illegal for a sweepstakes promoter to request upfront fees**. All foreign lotteries and sweepstakes are illegal as well. Any checks sent to you from the "promoter" will be counterfeit. The bank will hold your responsible for any funds spent.

Fake Employment Scam: These "jobs" are often listed online or in newspapers. You are sent what appears to be a legitimate check. You are instructed to cash the check and wire transfer funds to someone as your first "job" assignment. These checks are counterfeit . The bank will hold you responsible for the amount of the returned check and the fees. Furthermore, you may have provided personal information to the scammer which could result in identity theft.

Fake Check Scam: While attempting to sell an item online, the "buyer" sends you a check for more money than as requested for the item. The "buyer" claims the extra money was to be wired to a "shipping company" or explains it was a mistake and asks you to wire the money back. These checks are counterfeit and you will be responsible to the bank for the check and the fees. This tactic is often used for rental properties listed online as well.

Card Member Services Scam: The robo call (with the names "Rachel" or "Carmen" often used) claims that your credit card interest rates can be reduced or debt can be consolidated. You are asked personal financial questions and for your credit card numbers. You will either be enrolled in an expensive debt consolidation service or your credit card numbers will be used for unauthorized purchases.

Please note: This is not an all inclusive list of the scams being perpetrated on Kentuckians. There are many more.

BEWARE: If you receive funds from people you do not know and are asked to wire the funds to another person, you are serving as what law enforcement refer to as a **"mule".** The scammer is using you to transfer funds illegally. You may be held responsible for these transactions! Don't participate in this activity!

INFORMATION TO KNOW

The National Do Not Call Registry Or List:

The Do Not Call Registry can reduce the number of **unwanted sales** calls you receive **by legitimate businesses**; however, it does **not** block calls, **nor does it stop** all unwanted calls due to exemptions in the law. You may still receive debt collection calls, political calls, charitable calls, informational calls, or telephone surveys. **Additionally, the registry does NOT prevent scammers from calling you**. This is often a misconception that consumers have who are on the no-call registry. You may enroll on the National Do Not Call Registry at 1-888-382-1222. Detailed information about the Do Not Call Registry is available at www.donotcall.gov.

"Spoofing":

Scammers use current technology that makes it easy for them to "spoof" the caller ID information so that the phone number that appears on your caller ID probably isn't real. The number may appear to be from a legitimate agency, organization, or even your OWN phone number. Scammers use "spoofing" technology and internet based phone lines to make their calls from overseas. This "spoofing" technology makes it very difficult, if not impossible, for regulators to track the scammers.

It is advised that you NEVER return the phone call of suspicious numbers on your caller ID or Never return a call from suspicious messages left on your answering machine. Returning calls and interacting in any way only validates that your phone number is an active, useful phone line and will probably lead to more unwanted calls.

Call Blocking:

If you get repeated illegal calls from one particular number, contact your phone company to inquire if the number(s) may be blocked, but ask if there is a fee for this service. You may also research other call blocking solutions that block unwanted calls. Many are offered online or through smartphone apps. Make sure to read online reviews for effectiveness and costs.

Identity Theft:

Identity theft occurs when someone uses your personal information to open credit accounts, take out loans, apply for utilities or government benefits, or files taxes using your social security number. Scammers may contact you claiming to have your information, but this is not necessarily considered identity theft until the information is actually used to obtain credit or services without your consent or knowledge. You should, however, take precautions to protect yourself from identity theft if you suspect your information has been compromised .

If you have provided personal information to what appears to be a scammer, you should obtain a copy of the **Identity Theft Victim's Kit at www.ag.ky.gov.** or the **Federal Trade Commission's booklet on identity theft at www.ftc.gov/idtheft** . These resources will provide steps on how you can protect yourself.

Other Helpful Information:

Attorney General's Consumer Protection Hotline: 1-888-432-9257.

The Federal Trade Commission (FTC) : This agency also collects complaints and information on scams and makes them accessible to law enforcement. Any scam you encounter should also be reported to the **FTC at 1-877-382-4357 or www.ftc.gov.** The FTC also provides a good source of consumer information on their website as well.

Internet Concerns: Crimes perpetrated online should be reported to the Internet Crime Complaint Center at www.ic3.gov .

If You Lost Money To a Scam: Immediately contact the money service provider (such as Western Union, MoneyGram, i-Tunes, Green Dot, your credit card company, or financial institution), to report that the transaction was a scam and ask if the transaction can be canceled!