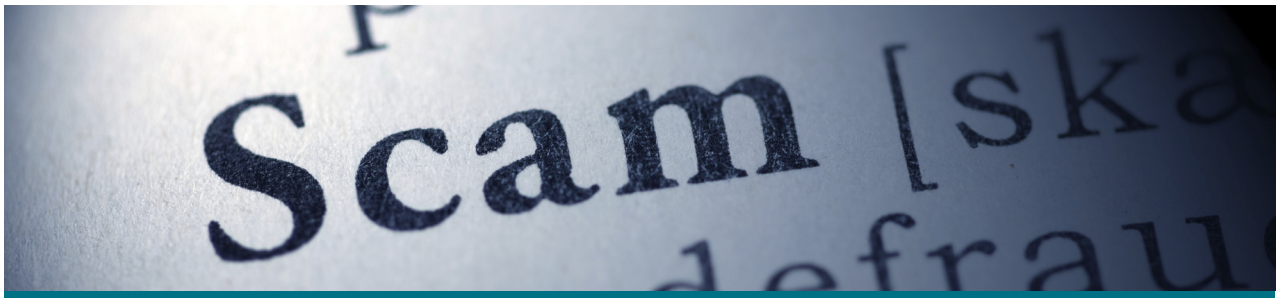
Investigator Tips



The Scams du Jour

Be on the Lookout—Avoid these Scams

Scams—a seemingly persistent threat—might be avoided if you are familiar with the scammers' tactics. Here are some of the scams currently circulating that the licensed private investigators at Kroll want you to be aware of:

- **Grandparents Targeted by Phony Debt Collectors.** The Federal Trade Commission (FTC) is alerting consumers to phony debt collectors calling people and claiming that they are collecting on a debt owed by a grandchild of the call recipient. The caller threatens to have the grandchild arrested or fired from their job and tells the grandparent that they can prevent this by sending money. Unless you co-signed on a loan, you are not responsible for anyone else's debt, even family members. Hang up if you receive any calls like this.
- **Calling Yourself?** If you receive a phone call and your caller ID service your own phone number is placing the call, the FTC advises to ignore the call. The caller is a scammer making an illegal robocall. If you answer and press a button to be removed from the call list or to speak to a person, you've simply validated your phone number and you will receive more calls of that type.
- **Delivery Notice Postcard and Phone Call.** Have you received a postcard reporting a failed delivery to your location? This is a scam that is very common and often perpetuated by email. However, recently we've heard of consumers receiving a postcard indicating there was a failed attempt to deliver a package that was followed by automated phone call with a similar message. This double notification might seem to legitimize the message but in reality this is a scam to convince you to pay for something you didn't request.
- **Computer Held for Ransom.** The Better Business Bureau (BBB) recently alerted consumers to the threat of computer ransomware. This is a virus that makes your computer unusable by encrypting the files until you pay the ransom which can be $200 to $10,000. The BBB offered the following advice:
  - Use antivirus software and a firewall
  - Enable pop-up blockers
  - Back up the content on your computer

Scams aren't always attempts to steal your identity but they certainly could lead to it. The scammer is ultimately after money and might try to convince you to share your personal information which they then use to commit identity theft for financial gain.

If you encounter a situation you are concerned might be a scam, contact IDShield during normal business hours.

MEM-115-2015-07-10

A service of the Investigators of Kroll. These materials are derived from the research and discovery activities of Kroll Fraud Specialists and Licensed Investigators, and have been gathered from personal, historical, and aggregated experience performing specialized restoration services on behalf of Identity Theft victims. While believed to be accurate, these materials do not constitute legal advice, and are not guaranteed to be correct, complete or up-to-date. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into a language or computer language, in any form by any means, electronic, mechanical, optical, chemical, manual or otherwise, without the express written consent of Kroll. These materials are provided for informational purposes only.