

SCS Connection

Southern Capital Services, Inc.
Registered Investment Advisor Since 1982

June 2017 • Volume: 25 • Issue: 6



You Can Protect Yourself from Fake Check Scams

by the Financial Industry Regulatory Authority

We at Southern Capital Services are reproducing an article that was recently issued on the FINRA (Financial Industry Regulatory Authority) website. FINRA has received a number of calls recently from individuals who have received unexpected checks, some from organizations whose names are household words. To those callers, we offer a concise response: Don't cash the check, it's almost certainly counterfeit.

In many instances, the name of a real company appears on the check, as well as real account and routing numbers. The common variety of this scam includes instructions to deposit the check in your bank account and then almost immediately transfer a portion of the money to someone else. Days later, your bank informs you that the check was counterfeit and that you are liable for the amount withdrawn, usually several thousand dollars. You've been scammed.

A variation of this scam simply delivers a check to your door, by registered mail or other delivery method that requires a signature. No instructions accompany the check—but FINRA suspects that once you deposit the check, you may further entangle yourself with the fraudster. For example, you might be liable for the amount of the counterfeit check, your endorsement might give your account information to fraudsters, or you could receive follow-up attempts to phish for personal financial information—or some combination. Here are some of the most common scams that involve fake checks.

Mystery Shopping Scam

Fraudsters lure victims by posting ads for mystery shoppers in job classifieds, such as on the popular Web site Craigslist (www.craigslist.org). When victims respond to the ads, they are led to believe that they have been hired as mystery shoppers to

evaluate the services of money transfer companies, such as MoneyGram. Victims are then sent checks that appear to be from legitimate companies—including FINRA—and instructed to deposit the checks in their bank accounts, then withdraw most of the money and wire it to someone else—often a purported fellow mystery shopper. Victims are told to keep several hundred dollars of the money as payment. When the checks are later discovered to be phony, the banks reverse the deposit and the victims are left liable for the money withdrawn, usually several thousand dollars.

Modeling Scam

Typically this scam starts with a victim responding to an online posting—or the victim may have posted information online, such as with a modeling clearing house. Either way, the victim eventually gets "hired" by the fraudsters to model and receives an email with instructions. Similar to the mystery shopping scam, the victim then receives a legitimate looking check and is told to cash the check, wire some portion of the proceeds to a third party—such as a "supervising crew"—and keep the remainder as payment.

Unexpected Check Scam

While it is possible that an event triggers the delivery of a "surprise" check to your door, such as responding to an online job or merchandise posting, a handful of potential victims who received fake checks and called us said they neither suspected nor recalled such an interaction. As mentioned above, the check may arrive with no instructions or additional information and, once deposited, your bank will likely require you to return any amounts disbursed if the check bounces—plus pay bounced check or other fees. In addition, you may leave yourself open to follow-up calls or emails that phish for personal financial information. If the fraudster receives or has access to the image of the cashed check, your endorsement might also reveal your bank account number.

Here's How You Protect Yourself

To avoid fake check scams, **follow these tips:**

Don't "keep the change." No legitimate company will overpay you and ask that you wire the difference back to the company or to some third party. Be extremely wary of any offer—in any context—to accept a check or money order in an amount greater than you are owed.

Don't cash the "unexpected" check. Companies rarely if ever send checks that don't include some explanation of why the check was issued. Unless you are expecting the check—and you are absolutely certain it is meant for you—do not cash it.

Call the company directly to verify the check. Remember that some fake checks will have a legitimate company's actual account number with the correct bank routing number. Call the company directly to verify the check, using a telephone number you obtain on your own from directory assistance. Do not use any telephone number that appears on the check or in any instructions you receive.

Know the hallmarks of fraud. Fake check scams typically have a number of red flags, such as:

- **Typos:** Watch out for online postings or emails that are riddled with typos and poor grammar.
- **Mismatched names:** Compare the name of the person or company posting the opportunity with the name on the check you receive—and beware if they don't match.
- **Pressure to act quickly:** Be aware that it can take 10 days or even more for your bank to determine that a check is counterfeit. Don't wire or transfer funds until you have verified with your bank that the check has cleared—even if the bank allows you to withdraw the money sooner.

If you receive a suspicious check, be sure to contact one or more of the following organizations right away: your local police, the Internet Crime Complaint Center (a partnership between the FBI and the National White Collar Crime Center), or the U.S. Postal Inspections Service (if the check arrived by U.S. mail).