



Beware of Fake Checks

Protect yourself from fake check scams with these tips from FDIC Consumer News

Even in today’s digital and mobile world where electronic money transfers are common, consumers and businesses may still prefer the assumed security of paper cashier’s checks or official bank checks for large or major payments. Recipients generally prefer one of these checks over a personal check because the financial institution presumably has already collected the funds from the party purchasing the cashier’s checks or official bank checks. This means the payment is guaranteed, unless the check is counterfeit, so there are risks to consumers and businesses from these types of paper instruments, as well.

Unfortunately, criminals have come to rely on their victim’s sense of “security” provided by cashier’s checks and official bank checks. Advanced graphics and printing technologies allow scammers to easily create fraudulent and hard-to-detect counterfeit checks in a matter of minutes, adding a sense of legitimacy to their scams. Fake checks can look so real that it’s very hard for consumers, or even bank employees, to detect.

Fake bank checks are typically used in scams where the scammer tries to get you to cash or deposit the check. Once it is deposited,

they ask that you send all or part of the proceeds back to them or to someone else (an accomplice) before the bank where it was deposited tries to clear or process the check for payment and realizes the instrument is fake. The scammer might ask you to return the funds in a number of ways: in cash, by writing a personal check, by loading it onto a pre-paid or gift card, or through some electronic means, such as a wire transfer, automated clearing house (ACH) payment, or a person to person (P2P) transaction.

If it is later determined that the check was counterfeit, you will likely be held responsible for the funds that were provided to the scammer, so it is important that you recognize the signs of a counterfeit check to protect yourself. Remember, fraud artists are constantly coming up with new ways to use fraudulent cashier’s or official bank checks in their scams. Here are three of the most common scams, and tips on how to detect whether or not you are being scammed.

1. Lotteries and Sudden Riches Scams

In these examples, the check recipients are told that they won a lottery—perhaps in a foreign country—or that they are entitled to receive an inheritance. The recipient is instructed that in order to “claim” their lottery winnings or inheritance, the recipient must first pay “taxes and fees” before they can receive their prize or money. A fake cashier’s check is sent, which the scammer asks the recipient to cash and then wire back the funds to cover the taxes and fees.

2. Online Auctions, Classified Listing Sites, and Overpayment Scams

Scammers might go to an online auction or classified listing site and offer to buy an item for sale, pay for a service in advance, or rent an apartment. The odd thing is that they might send you a cashier’s check for an amount that is higher than your asking price. When you bring this to their attention, they will apologize for the oversight and ask you to

quickly return the extra funds. The scammer's motive is to get you to cash or deposit the check and send back legitimate money before you realize that the check you deposited is fake.

3. *Secret or Mystery Shopper Employment Scams*

In these cases, the scammer advertises a job opportunity and claims to be "hiring" people to work from home. The "employee" might receive an official check as a starting bonus, and is asked to cover the cost of "account activation." The scammer hopes to receive these funds before the official check clears and the new employee realizes they've been scammed.

Another scenario involves an offer to work from home as a secret shopper to "assess the quality" of local money transfer businesses. The "employee" is sent a cashier's check and instructed to deposit it in their bank account and withdraw the amount in cash. They are then instructed to use a local money transfer business to send the funds back to the "employer" and "evaluate" the service provided by the money transfer business.

How to Spot a Fake Check

Determining whether a cashier's check or bank check is legitimate is difficult just by physical inspection. However, there are some things you can do to help identify a fake check:

- Make sure the check was issued by a legitimate bank. While some counterfeit checks will include a legitimate bank's name, a fake name is a sure giveaway. FDIC BankFind allows you to locate FDIC-insured banking institutions in the United States.

- Check with the bank that supposedly issued the check to make sure it is real. Make sure you look up the phone number on the bank's official website and don't use the phone number printed on the check (that could be a phone number controlled and answered by the scam artist). Next, call the official number and ask them to verify the check. They will likely need to know the check number, issuance date, and amount.
- Consider how and why you received the check. If someone you don't know initiated the payment, be skeptical and proceed cautiously. Scammers often communicate with their victims via e-mail or text message. Their communications may contain poor grammar and spelling errors.
- Look where the check was mailed from-- if the postmark is not the same as the city and state of the "supposed" issuing bank, it might be an indication the check is fake. Be especially cautious if it was mailed from overseas.
- Determine if the amount of the check is correct and as expected. Fake checks are often made out for more than the agreed upon amount. This is intended to coax the person receiving the check into wiring the overpayment back to the scammer.
- Official checks usually contain watermarks, security threads, color-changing ink and other security features. While scammers are able to sometimes copy these security features, the quality is often poorly executed.

What to Do if You Are Scammed

If you think you've been targeted by a counterfeit check scam, report it immediately to any of the following agencies:

- The Federal Trade Commission at <https://www.ftccomplaintassistant.gov/>.
- The U.S. Postal Inspection Service at <https://www.uspis.gov/> (if you received the check in the mail).
- Your state or local consumer protection agencies. Visit www.naag.org for a list of state Attorneys General.
- For possible online crimes involving counterfeit checks and money orders, file an online complaint with the Internet Crime Complaint Center (a joint project of the FBI and National White Collar Crime Center) at <http://www.ic3.gov>.

In addition to notifying the bank whose name is on the check, you can notify the website or online service where you encountered the scammer (for example, the online auction website or job posting website), so they can block them from utilizing their services in the future.

For more help or information, go to www.fdic.gov or call the FDIC toll-free at 1-877-ASK-FDIC (1-877-275-3342). Please send your story ideas or comments to Consumer Affairs at consumeraffairsmailbox@fdic.gov

