



# Check Fraud

---

Contact: Sarah Grano, ABA Public Relations (202) 663-5470 or [sgrano@aba.com](mailto:sgrano@aba.com)

## **Consumers' funds are protected against fraud.**

- If you are a victim of check fraud, the bank will make sure you don't lose a single penny.
- Banks typically provide provisional credit to the customer while an investigation takes place.
- Even though customers' funds are protected, they should still take precautions (see consumer tips below). Like being rear-ended in a car accident, it may not be your fault, you may not have to pay for the repair, but it is important to take the steps to ensure your car and safety are not in jeopardy – the same applies with fraud.

## **Bank systems prevent the majority of check fraud attempts.**

- Banks' prevention systems stopped about 85 percent or \$11 billion in fraud attempts in 2014, according to ABA's Deposit Account Fraud Survey Report (2015).
- Attempted check fraud at U.S. banks totaled \$6.8 billion in 2014. Actual bank losses totaled \$615 million in the same year, down from \$648 million in 2012. The number of fraud cases increased to 565,303 from 474,096 in 2012.
- Employee training is still one of the most effective security measures. Other prevention systems include fraud detection software, hold policy, large dollar item review and new account screening.

## **Beware of fake "check and wire" scams.**

- The cashier's check or "advance fee" fraud became more prevalent with the advent of online auction sites and classified ads.
- Here's how it works: A fraudulent buyer offers to send a cashier's check or money order for an amount much larger than the value of the auctioned item and asks that the seller wire back the difference. Once the seller receives the cashier's check, he or she deposits it, and then wires the leftover sum to the buyer. As many as 10 days later, the bank may determine that the cashier's check was fraudulent. Unfortunately, by then the seller has lost their money and merchandise to a scam.
- No legitimate company will offer to pay by arranging to send a check and asking the seller to wire some of the money back. If that's the pitch, it's a scam.
- If a stranger wants to send you payment for something, insist on a check for the exact amount, preferably from a local bank or one with a branch in your area.

## **Ensure a check has "cleared" to be most safe.**

- Under federal law, banks must make deposited funds available quickly – usually within two days. But just because you can withdraw the money doesn't mean the check is good, even if it's a cashier's check or money order. Forgeries can take weeks to be discovered. Be sure to ask if the check has *cleared*, not merely if the funds are available.
- Consumers and businesses are responsible for the checks they deposit, because they know best the origin of the check. Banks are required to make

# Check Fraud

---

(continued)

funds available within two business days; however, that does not mean a check has cleared and is not fraudulent. It can take several weeks for a check to clear or be returned as fraudulent.

- If you are uncertain a check is good, wait until the check has “cleared” to spend the money.

## **Consumer Tips to Prevent Fraud:**

- **Don't share your secrets.**  
Don't provide your Social Security number or account information to anyone who contacts you online or over the phone. Protect your PINs and passwords and do not share them with anyone. Use a combination of letters and numbers for your passwords and change them periodically. Do not reveal sensitive or personal information on social networking sites.
- **Shred sensitive papers.**  
Shred receipts, banks statements and unused credit card offers before throwing them away.
- **Keep an eye out for missing mail.**  
Fraudsters look for monthly bank or credit card statements or other mail containing your financial information. Consider enrolling in online banking to reduce the likelihood of paper statements being stolen. Also, don't mail bills from your own mailbox with the flag up.
- **Use online banking to protect yourself.**  
Monitor your financial accounts regularly for fraudulent transactions. Sign up for text or email alerts from your bank for certain types of transactions, such as online purchases or transactions of more than \$500.
- **Monitor your credit report.**  
Order a free copy of your credit report every four months from one of the three credit reporting agencies at [annualcreditreport.com](http://annualcreditreport.com).
- **Protect your computer.**  
Make sure the virus protection software on your computer is active and up to date. When conducting business online, make sure your browser's padlock or key icon is active. Also look for an “s” after the “http” to be sure the website is secure.
- **Protect your mobile device.**  
Use the passcode lock on your smartphone and other devices. This will make it more difficult for thieves to access your information if your device is lost or stolen. Before you donate, sell or trade your mobile device, be sure to wipe it using specialized software or using the manufacturer's recommended technique. Some software allows you to wipe your device remotely if it is lost or stolen.
- **Report any suspected fraud to your bank immediately.**