

Cashier's Check Fraud

The Latest Wrinkle

by Kirk Johnson

Just when you think you've heard it all, some clever thief comes up with a new scheme to invade your business and attack its hard-earned profits.

A recent study from the Association of Certified Fraud Examiners (ACFE) shows that a typical organization loses a median estimated 5 percent of annual revenue to fraud. While the most common cause of business fraud is dishonest employees, a growing epidemic of cashier's check fraud is affecting businesses at an alarming rate. Hardest hit are those doing business over the internet.

Here's how it works

A large ticket item is placed for sale on the internet. A buyer offers to purchase the item and pays with a cashier's check (sometimes provided by a third party who owes the buyer money). The seller receives the check and finds that it is written for more than the advertised price of the item. When asked, the buyer may give one or more reasons for the overpayment, including transportation charges, misunderstanding of terms, an accounting error, etc. The buyer then suggests that the seller deposit the check and simply wire the excess amount to the buyer (note: a wire transfer is an electronic, real-time vehicle that allows banks to transfer funds to each other in a timely and safe manner¹). Often, a buyer will explain that he or she needs the money wired due to adverse circumstances (i.e., problems with the IRS, poor health or a family death).

In a recent local case, multiple large-ticket items were sold. When the seller received the check, it was written for the correct amount. A short time later, the buyer called and cancelled one of the items, asking that the refund be wired to him.

Gotcha!

In both of these cases, the seller, wishing to be paid, deposited the cashier's check. When the seller's bank verified the deposit, the funds were made available and the seller sent

the wire to the buyer. Sounds simple—no problem—right? Wrong. The problem is that this is a scam. *The cashier's check was counterfeit*, although it looked authentic enough to fool the bank. By law, the bank must make the money available to the seller quickly, usually within a couple of business days. Because the seller is ultimately responsible for the validity of the check, when the bank finally discovers that the check is fraudulent—perhaps weeks later—it can (and does) reverse the seller's deposit, subtracting the amount of the cashier's check from the seller's account. Meanwhile, the wire transfer has been sent to the "buyer" (thief) and the money is, sadly, long gone.

Is there any recourse?

Fraud has many variations and thieves constantly invent new scams. Unfortunately, there is no form of insurance available to cover this type of loss. The best way to protect your identity and your assets from fraud is through education and self-awareness. Learn more about the types of scams being circulated and how to protect yourself from them. If you have questions about banking transactions, talk to your banker. The following steps are good guidelines for anyone doing business over the internet:

1. If you don't know the buyer, be wary if he or she wishes to pay by cashier's check instead of through a service like PayPal. If a deal seems too good to be true, it probably is. Ask yourself "Why would a person I've never met ask me to do this?" If you can't come up with a reasonable explanation, you're wise to ask more questions before taking action.
2. If you receive a cashier's check and are asked to return money by wire, always call the issuing bank to validate the cashier's check. Do not call a telephone number provided by the buyer, because you'll probably just be calling the

thief. Get the phone number from an independent source, such as directory assistance or the internet.

3. Never send merchandise or refund money from a transaction of this sort until the cashier's check has been paid by the issuer, even if it takes a month. Change your accounts receivable and payable policies, if necessary, to prevent this from happening, and make certain your accounting staff is aware of this scam.
4. Remember that you have the right to refuse the sale. If the buyer will not agree to use an online payment service and insists that you accept a check for more than the selling price, it's OK to walk away. Likewise, pressure by the buyer to "act right now" should alert you that the transaction may not be safe. If a payment is good today, it should be good after the check clears the issuing bank. A buyer who's not willing to wait may have something to hide.²

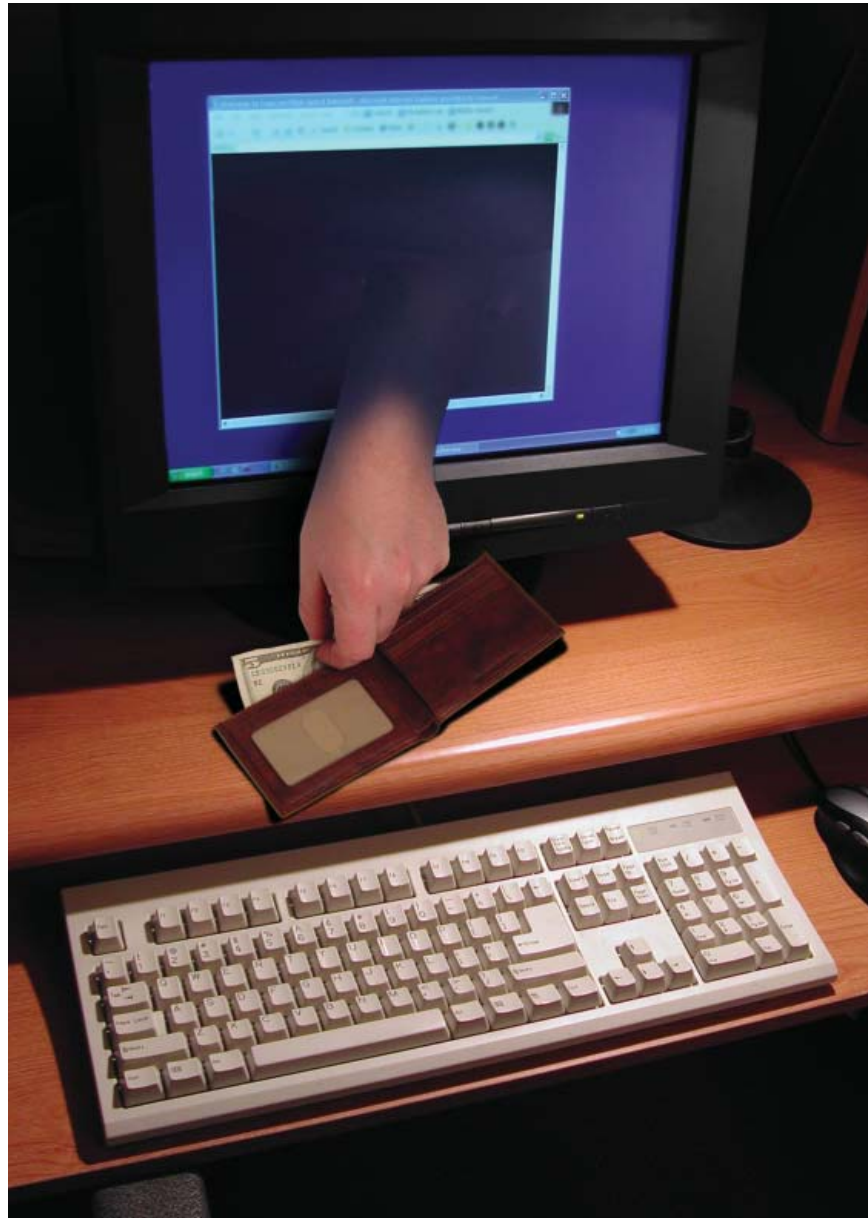
If you believe you have been the victim of a check overpayment scam, notify your bank immediately and follow up by filing a complaint with each of the following entities:

- the Federal Trade Commission at www.ftc.gov or by calling 877.FTC.HELP
- the Federal Bureau of Investigation's Internet Fraud Complaint center at www.ic3.gov
- for mail fraud, the U.S. Postal Inspector Service at 888.877.7644; write to U.S. Postal Inspection Service, Office of Inspector General, Operations Support Group, 222 S. Riverside Plaza, Suite 1250, Chicago, IL 60606-6100; or e-mail through the website, <https://postalinspectors.uspis.gov/contactUs/filecomplaint.aspx>

If you are unable to resolve the problem with your bank, you can contact the Office of the Comptroller of the Currency's Customer Assistance Group by calling 800.613.6743 or via e-mail at customer.assistance@occ.treas.gov.³

The following additional websites offer more information about fraud and scams:

- Is it urban legend or fact? Check it out at www.snopes.com.
- At the FDIC's Federal Citizen Information Center website, you can find helpful tips and sign up for e-mail fraud and scam alerts. Visit <http://pueblo.gsa.gov/>.
- The American Bankers Association website offers guidelines for avoiding cashiers check fraud. Check it out at www.aba.com/ABAEF/cashierscheckfraud.htm.



¹ "Federal Reserve Wire Network" InvestorWords.com. WebFinance, Inc. July 15, 2008 <http://www.investorwords.com/6516/Federal_Reserve_Wire_Network.html>.

² The Federal Trade Commission website, "Check Overpayment Scams: Seller Beware," accessed on July 15, 2008, <http://www.ftc.gov/bcp/online/pubs/alerts/overpayalrt.shtm>

³ <http://www.occ.treas.gov/ftp/ADVISORY/2007-1.html>

Some information for this article was inspired by Cardinal Bank, a member of the Virginia Bankers Association, and is available at <http://www.cardinalbank.com/docs/2005CardinalCounterfeitChecksFYsk.pdf>.