Avoid Check-Washing Agitation

By Dawn Taylor, CFE

According to the recently released American Bankers Association 2009 Deposit Account Survey Report, check-related losses exceeded one billion dollars in 2008. One particular threat against deposit accounts is check washing, a scheme that is exceptionally easy to execute, but even easier to prevent through precautionary measures.

Check-washing enthusiasts, whether drug addicts, street criminals, or those facing tough economic times, begin their scheme by obtaining someone else's check, often through one of the following methods:

- Breaking into neighborhood delivery-and-collection-box units and apartment panels by prying open locks or removing entire units from their metal anchors.
- Driving or walking through neighborhoods, especially rural ones, and secretly inspecting outgoing mail left in curbside mailboxes.
- Waiting until U.S. Postal Service collection boxes fill up on Sundays or holidays, and then reaching inside to retrieve letters that haven't dropped down.
- Stealing checks, or having an accomplice steal checks, from businesses.

Washing a check is a fairly simple process, and checks that lack appropriate security features and are written in standard ballpoint or felt-tip pen make prime candidates for it. The clever criminal only changes the payee, leaving the amount intact with the hope that the account holder will not closely review his canceled checks. The result is a signed blank check that the thief can rewrite to suit his needs.

To facilitate washed-check cashing, sophisticated crooks keep laptops, digital cameras, laminating machines, scanners, and printers in their vehicles. These tools allow them to create false state-issued identifications (IDs). The less sophisticated readily obtain fake IDs "off the street," online, or through various store fronts. Armed with a fake ID, thieves can easily cash checks for a small percentage-fee at a check-cashing store. Another option for converting checks is to use them to purchase merchandise (especially big-ticket items from major retailers), later returning the merchandise for cash back. Crooks can also provide washed checks to co-conspirators, who then use their own ID or a fake one to negotiate the checks, keeping a portion of the proceeds.

Many banks and merchants take measures to protect against check-washing frauds. For example, banks often require nonaccount holders, those opening new accounts, and those purchasing cashier's checks and money orders to affix their fingerprints to the face of each check they cash. This way, in the event that the check is found to be fraudulent, evidence is readily available for a law enforcement investigation. Additionally, tellers and clerks generally are taught to spot distinguishable characteristics of washed checks.

Rather than leave your financial security in the hands of others, consider the following measures to minimize your risk of becoming a victim of a check-washing scheme and to detect a fraud sooner if it does occur.

Minimize the number of checks you write. Pay bills online using a secure computer. Most large banks offer this service, and many of them provide consumers with zero-liability protection for fraudulent transactions. Use a credit or debit card for purchases and for certain bill payments (e.g., insurance payments); credit and debit cards offer greater protection against fraud than do personal checks. Most large financial institutions offer zero-liability for consumers who are the victims of fraudulent debit and credit card transactions.

Only use checks that contain security features, including security ink and chemically sensitive paper, to protect against check washing. Other safety measures for checks that don't directly pertain to check washing, but are worth looking into, include watermarks, copy "void" pantographs, microprinting or high-resolution graphics, invisible and visible fibers, security screens, and three-dimensional reflective holostripes. Also, do not have your driver's license or Social Security number printed on your checks.

Use pens containing indelible black gel inks that, unlike dye-based inks, can't be easily removed with water or chemicals. These special gel pens are available from Avery, Pilot, Uni-ball, and other brands for $2 to $3 apiece at office supply stores.

Never use an unlocked mailbox for incoming or outgoing mail. Ideally, have incoming mail delivered to a Post Office Box, and drop off outgoing mail at the post office, preferably inside. At a minimum, put a lock on your mailbox.

Mail your bills safely. Don't leave mail in a mailbox overnight or drop it off for pickup on a Sunday or holiday. Make sure that any mail deposited into a box actually drops down into the box so that no one can reach in and remove it.

Do not leave rent payments in drop boxes. Mail or hand them to your landlord directly.

Strictly monitor your bank account activity. Review your bank activity for suspicious transactions as often as possible, preferably daily. Through online banking, you can view most transactions in real-time. View the front and back of cleared checks to verify that both the amount and payee are what you intended. Do not take for granted that because a check cleared for the correct amount, the intended recipient cashed it; otherwise, you risk finding out too late (e.g., after having a debt sent to collections or having an insurance policy canceled) that your check has been altered. Finally, reconcile your bank account often and address any discrepancies, keeping in mind that most financial institutions will only accept fraud claims within 30 to 60 days after a statement has been mailed.

Investigate any of the following:

- A call from a bill collector for a payment you know you mailed
- A check declined by a merchant when you have not bounced any checks
- A merchant notice about a bounced check you did not write
- A notice from a check verification company regarding a problem of which you were not aware

Reconcile your bank account monthly, if not more frequently, and address any discrepancies in a timely manner.

In the unfortunate event you or your client become the victim of check washing, proceed as follows:

- Report the crime to law enforcement, and obtain a copy of your police report and case number—to verify the crime, your bank may ask you to reference these items.
- Notify your bank, place any necessary stop payments, close compromised accounts, and request a refund of lost funds.
- Obtain a notice from your bank that the compromised accounts have been closed, and send (or have the bank send) copies of the notice, along with the police report, to any merchants or check verification companies that may have accepted a fraudulent check from your account.
- Request letters from any merchant involved that state that you are not responsible for the charges, and keep them on file for at least ten years.

- Contact the fraud units of each of the three credit reporting bureaus—Equifax, Experian, and TransUnion—and request that they place a fraud alert on your account.
- File a complaint with the Federal Trade Commission, an organization that can help you resolve the problems that result from check washing or refer you to other appropriate agencies and private organizations for further action.
