Fraud Prevention

Avoiding and Spotting Check Washing Fraud: Old Scam, New Tricks

While using checks for payment is falling out of practice, check fraud persists. According to the Financial Crimes Enforcement Network (FinCEN), suspicious activity reports (SAR) for check fraud at depository institutions increased by more than 200 percent between 2018 and 2021.

One common form of check fraud is check washing. Check washing is the process of erasing details from checks to allow them to be rewritten for a higher, fraudulent amount for deposit. Scammers may steal checks from blue U.S. Postal Service boxes, residential mailboxes, cluster mailboxes at apartments, and mailboxes in office or industrial buildings.

Business checks are a frequent target of check washing because business accounts usually contain more money, and businesses issue and receive a high volume of checks. Check scammers, however, also target personal checks, tax refund checks, and other government assistance checks.

Scammers are also using technology to wash checks. They scan the check, keep the signature in place, and use computer software to alter other data; for example, they may increase the amount and change the payee. Scammers may also copy and print multiple electronically washed checks for future use to sell to third-party scammers.

Since many check washing scams begin with checks that are stolen from residential, commercial, and U.S. Postal Service mailboxes, consumers and financial institutions can avoid check fraud by not mailing or receiving checks unless a traceable delivery method is used. Other options include using a bank's bill pay services to send electronic checks or sending money through other secure electronic means. Banks should make their customers aware if they have a program that will alert customers to the possibility of fraudulent checks. In the past, using difficult-to-erase gel pens was a preferred method for deterring check fraud; however, gel pens may not deter electronic forms of check washing.

View these additional resources on check washing fraud:

Federal Deposit Insurance Corporation (FDIC), **FDIC Consumer News: Beware of Fake Checks**
American Association of Retired Persons (AARP), **6 Ways You Can Thwart Check Washers**

Protecting Your Personal Information

Beware of Phishing Scams: Phishing attacks attempt to compromise consumer's personal identity data and financial account credentials. These schemes use e-mail to lead unsuspecting consumers to counterfeit websites. These false websites are designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords, and social security numbers. By hijacking the brand names of banks, e-retailers, and credit card companies, phishers often convince recipients to respond.

PLEASE REMEMBER THAT COUNTY SAVINGS BANK WILL NOT CONTACT YOU ASKING FOR ANY OF YOUR PERSONAL FINANCIAL DATA VIA E-MAIL. If you receive an e-mail of this sort, please do not respond to it. Please call us immediately at 610-521-1080 during normal business hours.

County Savings Bank takes your security seriously. Please take time to visit the following links for more information on how to protect yourself on the Internet.

How Not to Get Hooked by a "Phishing" Scam
Federal Trade Commission: What to Do If You're Personal Information Has Been Compromised

Note: When you click any of these links, you will be leaving the countysavingsbank.com website. Please refer to the Terms of Use and Privacy Policy of these outside websites. County Savings Bank is not responsible for the quality, delivery or timeliness of goods or services of outside websites.

Check your credit

Another source of protecting yourself from fraud is to check your credit. The government offers an annual free credit report from each of the three credit bureaus.
Visit https://www.annualcreditreport.com/index.action to learn more.

General Security

While anyone can fall prey to fraud and identity theft, many ways exist to minimize your risk. County Savings Bank provides these security tips so you can guard against fraud and protect your personal information.

Privacy

- Never give out personal information online or over the phone unless you have initiated the contact.
- Don't include information such as your driver's license or Social Security Number on your pre-printed checks.
- Avoid using easily guessed or learned information as your online password or personal identification number (PIN).

Safeguard Accounts

- Store new and cancelled checks in a secure place and shred unnecessary financial documents.
- Avoid writing your account number on envelopes or other items that may be thrown away later.

Protect Your Cards

- Choose passwords and personal identification numbers (PINs) that are difficult for others to guess.
- Use a different password for each of your online accounts.
- Do not share your IDs, passwords, or PINs with anyone.
- Change your passwords often.
- Keep a secure list of your card account and customer service numbers in case your cards are lost or stolen.
- If you are shopping online, don't provide your personal or financial information through a company's website until you have checked for indicators that the site is secure, like a lock icon on the browser's status bar or a website URL that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some scammers have forged security icons.
- Monitor your card transaction activity on your bank statements.
- Upon receipt of your card, ensure that you sign the back signature panel.
- To report suspicious card activity, or lost/stolen cards, please contact County Savings Bank Customer Service at 610-521-1080 during regular business hours. If there is suspicious activity during non-business hours please call 1-800-554-8969.

Protect Your Mail

- If you stop receiving bills, statements or other monthly mailings, or if a bill is not received when expected, contact the issuing company immediately, this may be an indication that your mail is being intercepted.
- Promptly collect incoming mail and use a locking mailbox if possible.
- Send outgoing mail from a secured mailbox or a post office; try to avoid leaving outgoing mail in your home mailbox.
- Shred all unwanted pre-approved offers for credit cards, convenience checks or loans.

ATM Safety

- Shield the ATM keypad with your hand or body while entering your PIN.
- If you notice anything suspicious or that seems unsafe, such as the lighting around the ATM not working, use another ATM or return later.
- Beware of skimming devices which generally will stick out a few extra inches from an ATM. If something looks suspicious, find another ATM. Don't fall for a poor fitting device (or a sticker or sign that says 'Swipe Here First' or 'Use This Machine Only').
- Immediately put away your card or cash.
- Be aware of nearby strangers.
- Never leave your transaction statement behind.
- If a machine keeps your card, call the bank immediately and report it.
- Treat your ATM card like cash. Keep your eyes on your card; don't let a merchant walk off with your card even for a few seconds.
- If you use a drive-up ATM, make sure all doors are locked and all other windows are rolled up.

Personal Information Protection

- Carry only necessary identification. Do not carry your Social Security Card with you.
- Be cautious of telephone and door-to-door solicitations.
- Don't leave personal information in your car. It's even more valuable than your stereo.
- Shred unnecessary financial information immediately.
- Check your credit report annually.

Seven Practices for Safer Computing

Access to information and entertainment, credit and financial services, products from every corner of the world even to your work is greater than earlier generations could ever have imaged. Thanks to the Internet, you can order books, clothes or applications online; reserve a hotel room across the ocean; download music and games; check your bank balance throughout the day; or access your workplace from thousands of miles away.

The flip-side is that the Internet and the anonymity it affords also can give online scammers, hackers and identity thief's access to your computer, personal information, finances and more.

With awareness as your safety net, you can minimize the chance of an Internet mishap. Being on guard online helps you protect your information, your computer, even yourself. To be safer and more secure online, adopt these seven practices.

1. Protect your personal information. It's valuable.

2. Know who you’re dealing with.
3. Use antivirus and personal firewall software and update both regularly.
4. Be sure to set up your operating system and Web browser software properly, and update them regularly.
5. Protect your passwords.
6. Back up important files.
7. Learn who to contact if something goes wrong online.

Parents

Parental controls are provided by most ISPs, or are sold as separate software. No software can substitute for parental supervision. Talk to your kids about safe computing practices, as well as the things they’re seeing and doing online.