Democracy Dies in Darkness

Why mailing a paper check has become so risky

Criminals use chemicals to “wash” away the recipent's name and dollar amount, and then rewrite the check to themselves.

June 17, 2026

Column by Michelle Singletary

We’ve become so used to high-tech cybercrime that we may sometimes forget about the vulnerability of our mailboxes.

But an old-school, low-tech scam is surging and is more than enough reason to avoid or limit writing paper checks altogether. And the recent predicament faced by a California couple who reached out to me shows how challenging it can be to retrieve money after a check’s been altered.

According to a joint warning from the FBI and the U.S. Postal Service, check fraud is skyrocketing. Federal data shows that reports of check fraud nearly doubled from 350,000 in 2021 to 680,000 in 2022.

It’s gotten so bad that the agencies recommend considering e-checks, ACH automatic payments and other electronic or mobile payments.

In 2010, there were just over 2,200 high-volume mail theft attacks, and by 2023, that number had skyrocketed to over 49,000, a “2,000 percent explosion,” Frank Albergo, president of the Postal Police Officers Association, said last summer during testimony before a House subcommittee.

“This is not about lost birthday cards anymore,” Albergo said. “We’ve entered an era of organized postal crime.”

Criminals use everyday household chemicals like acetone or bleach to “wash” away the payee’s name and dollar amount, allowing them to rewrite the check to themselves.

The California couple recently learned this the hard way after getting a notice from the Internal Revenue Service that they had missed their quarterly tax payment and now owed $12,000 plus interest and penalties.

The couple, who spoke on the condition of anonymity to protect their privacy, were shocked and puzzled. They knew they had paid on time.

“We looked at our online Chase statement, and the check had cleared,” the wife said in an email.

But when they pulled up the scanned image of the cleared check, they saw that someone had changed the “pay to the order line,” erasing the IRS as the recipient and replacing it with an individual’s name.

This isn’t limited to personal checkbooks. Fraudsters are going after business payments, tax refunds and checks related to government assistance programs, such as Social Security and unemployment benefits, according to the Financial Crimes Enforcement Network.

If your tax refund from the government is stolen and cashed, there’s a process to report the theft. However, recovering from a stolen personal check can be much harder.

Once they realized what had happened, the California couple contacted Chase. But they were told they had missed the deadline to report the fraud. The check had been stolen and deposited a year earlier.

Still, they persisted and found that the check had been deposited by another Chase customer.

“We feel the bank was negligent in this transaction and owes us reimbursement,” the wife said. “I feel we could make a good argument, 60 days or not.”

They reached out to ask if I could help.

Chase’s initial refusal was technically legal. The deadlines for reporting and recovering funds are primarily governed by your bank’s deposit agreement and the Uniform Commercial Code. If you miss the window, the liability usually falls on you.

However, given how pervasive fraud is, financial institutions should do whatever they can to do the right thing, even when they aren’t in the wrong.

After I inquired about the case, Chase reinvestigated the situation. The bank was able to trace the fraudulent account to which the stolen money had been routed. It turned out there was still about $11,000 sitting in that account, enough to almost entirely reimburse the victimized couple.

This couple was incredibly fortunate. Most of the time, the money is long gone before a customer or bank discovers the scam.

“We’re pleased we were able to resolve this matter,” Chase spokesman Jerry Dubrowski said in an email.

It was a win for this couple, but a warning for the rest of us.

“We encourage customers to avoid mailing checks and to use safer payment methods, such as electronic transactions,” Dubrowski said. “If a customer must use a check, they should review their monthly statements to ensure payments are properly recorded.”

The primary reason washed checks clear successfully is that modern bank processing relies heavily on automation and speed.

Unless a check is manually inspected for evidence of tampering — such as chemical staining, discoloration or a mismatch between the signature’s handwriting and the payee line — a fraudulent check can clear, and the funds will be transferred directly to the thief.

If you still choose to write a check, the FBI and the Postal Service offer these tips.

Protect your mail

- Get your mail as soon as you can. Definitely don’t let it sit in your mailbox overnight. And avoid leaving outgoing mail in unattended home mailboxes with the red flag up.
- Use the Postal Service hold mail service if you are heading out of town.
- Buy security envelopes so thieves can’t see there’s a check inside.
- Go inside the post office to drop off outgoing mail. If you absolutely must use an outdoor blue box, don’t deposit a check after the day’s final pickup time.

Protect your check

- Write checks with permanent, indelible black gel ink. Standard ballpoint pen ink washes off easily; gel ink traps itself in the paper fibers.
- Don’t leave blank gaps on the payee or dollar amount lines where a thief can sneak in extra words or numbers.
- Don’t just check your bank balance online. Look at the actual digital image of your cleared checks to confirm the payee’s name wasn’t altered.
- Check your online banking activity frequently. Verify everything about it.

- If a check you wrote is taking longer than usual to clear, or if you spot any missing funds, contact your bank immediately.
- Order checks that have security features, such as microprinting, watermarks or chemically reactive paper that bleeds when touched by bleach or acetone.

It’s unfortunate we have to become forensic investigators just to pay our bills. But as criminals continue to exploit old-school vulnerabilities, we must be overzealous in protecting ourselves.