

Writing Checks Can Be Risky. Here's How To Protect Yourself.

 [nytimes.com/2024/01/07/business/check-fraud-prevention.html](https://www.nytimes.com/2024/01/07/business/check-fraud-prevention.html)

Tara Siegel Bernard

January 7, 2024

Typewriters vanished, and then cassette tapes and encyclopedias did, too. But paper checks are one piece of our analog past that persists.

American consumers and businesses wrote 11.2 billion checks in 2021, far fewer than the 42 billion written at the start of the century. Despite the rapid decline, check fraud is exploding — costing financial institutions billions and throwing many check writers' finances into disarray.

After my colleague Ron Lieber and I wrote about rising check fraud, worried readers wrote to us with questions: Is there a safer way to write checks when we must? What about digital payments — aren't they susceptible to fraud, too?

Many Americans still write checks to pay rent or avoid credit card fees. They also may cling on to checks for cultural reasons or for psychological ones — for example, because writing them out is a manual process, almost like using cash in an increasingly cashless society.

So the little rectangular slips of paper press on, even as digital payment methods like Venmo and Zelle have achieved verb status — just Venmo me! — and continue to gain in popularity.

Here are some tips on how to transact business as safely as you can, in both the paper and digital realms.

Are there certain practices to keep in mind when writing checks?

This is a return to basics, but it's worth revisiting: When writing the payee's name, use the entire line or draw a line to the end so that nobody can add an additional name or more information. Do the same when you write the amount in words and numbers.

Signing your checks the same way every time is also essential. We've heard from readers whose check payments were frozen because the handwriting was deemed suspicious. That's a good thing, but it can send your financial life into a tailspin if you become locked out of your accounts because of an investigation.

And remember, when you write a check out to "cash," anyone can use it — so proceed with caution or avoid doing that altogether.

What's the best pen to use when writing checks?

First, let's back up and explain why pens matter: Thieves steal checks from the mail and then "wash" the ink off using materials as basic as nail polish remover, leaving the signature untouched. Criminals then usually rewrite the checks to their own accounts or sell the checks on the dark web.

No pen is completely fail-safe, but gel pens are the safest bet: Unlike ballpoint pens, whose ink sits on top of the paper, gel is more difficult to wash because the ink penetrates the fiber of the paper, according to Karen Boyer, a check fraud expert.

Are there any banks that have extra protections in place, like flagging a weird check to customers by sending a text message?

There are. Not all banks do this, but Capital One, for example, contacts customers via text, email or phone when it notices an "unusual check" and wants to ensure it's legitimate (similar to what credit-card issuers often do). Customers can also create alerts in the bank's mobile app to receive emails when checks are paid.

Bank of America will reach out to customers when it detects an out-of-character check as well. Contact your bank to see if it offers anything similar, and make sure it has your preferred method of communication on file.

Should I keep a separate account just for check writing?

Some readers suggested this strategy, and it seems to be a smart one for people who regularly write personal checks. By keeping a separate account with enough to cover the checks you write, you cap any potential losses.

Richard Stutman of Boston turned to that strategy after one of his checks was stolen and washed even though he had made sure to mail it from inside his local post office. He holds two checking accounts: One is used for direct deposits and online banking, while the other holds only a small balance to cover checks that he can't avoid writing. "It's a small nuisance, but I have the comfort of knowing that I never have more than a few hundred dollars at risk," he said.

Should I stop mailing checks?

The United States Postal Service has said that depositing mail inside your local post office or handing it to a postal carrier is your safest bet.

If you must mail an important or large payment, it might be wise to pay for tracking — certified mail, for example, or a signature confirmation upon delivery — as a safeguard.

But here's something you absolutely shouldn't do. Some residential mailboxes have little flags that, when raised, signal to postal carriers that you'd like them to collect your outgoing mail. That's an invitation to thieves, indicating that there may be a valuable check inside.

Empty your mailbox frequently, and don't leave mail inside overnight.

Is the U.S.P.S. doing anything to address the spike in crime?

Yes. The Postal Service, along with the U.S. Postal Inspection Service, initiated a campaign last May to crack down on postal crimes, including attacks on its letter carriers, which have led to more than 630 arrests for robberies and mail theft.

You may have also noticed that the blue U.S.P.S. mailboxes that dot the streets have new features, like smaller slots, that make it more difficult to fish mail out. They have also begun to install electronic locks on mailboxes, replacing the old arrow locks that can be opened using keys and that provide access to all the mailboxes in a specific area. Those keys have become a hot commodity, stolen by criminals who have increasingly targeted mail carriers.

If your check has been stolen from the mail, the Postal Service urges you to report the theft as soon as possible by submitting an online complaint at www.uspis.gov/report or calling 877-876-2455.

Should I take pictures of the checks I put in the mail as proof?

It can't hurt. Customers who fall victim to check theft eventually see any stolen, altered checks (or fraudulent checks that a criminal has cooked up from scratch, using your information) in their online banking register. Having the original copy could help in an investigation should the need arise. (Unless, of course, the image is somehow stolen from your phone.)

Is there anything I should keep in mind when depositing a check, especially if I'm doing it remotely using my bank's mobile app?

Only endorse, or sign the back of, a check just before you're about to deposit it. And when you use mobile deposit, be sure to write "for mobile deposit only" below your signature. (Some banks' checks offer a box to tick if you are depositing the check remotely.)

Is a bank's online system the safest way to make payments? Or is it unsafe when it results in paper checks, even though the whole thing is supposed to be electronic?

Banks, without question, recommend their online bill-payment platforms over paper checks. These systems are highly secure, particularly when they already have your payees in their system and can send an electronic payment directly to them. But what happens if the payee cannot accept electronic payments?

That appears to vary by bank. If a bank does not know the payee, it generally sends a paper check on your behalf, but the checks may have your account number and other information on them, leaving them susceptible to fraud. They are sent from banks' mail rooms, which

may be more secure than a metal box on the street. But this method won't stop a thief from potentially plucking the check out of the box on the receiving end.

Some banks have made this process more secure. Chase's online bill-payment service, for example, sends checks on your behalf but without your account and routing number printed on them.

Why don't all banks do this? It's worth calling your institution to ask.

Can I cross out my account number from the bottom of the check?

Nope. Don't cross it out. The account number and routing number at the bottom of the check are used to deduct the money, telling the bank which account the funds belong to. Crossing it out could make the check unreadable and raise a red flag, said Jerry Dubrowski, a Chase spokesman. If you want to avoid sharing your account information, he suggested, use online bill payments.

What's the best way to make payments to charities or other organizations that charge fees if you use credit cards?

Making donations directly from your bank account is generally the most cost-effective option, according to Kevin Scally, chief relationship officer at Charity Navigator, a website that evaluates organizations. But even that can carry a small fee, which is why many people turn to checks.

Platforms like Venmo are increasingly an option, but Mr. Scally cautions that donors should never send funds to personal accounts — they should ensure that their transactions are directed to a verified charity account to receive a tax receipt.

He also said that using a credit card served as a "protection barrier against potential scams, allowing donors to file complaints and get their money back if they run into any red flags associated with the charity they donate to."

What about wedding and other occasional gifts?

Sending a monetary gift via Venmo or Zelle feels, well, transactional. If you choose to write a check, you can hand it to the recipient to circumvent the risks of snail mail.

Some couples register for "cash" gifts, which may be earmarked for a honeymoon or a down payment. Unfortunately, many of these gift payments carry fees. Zola doesn't charge any if gift givers pay through Venmo.

Are there any extra protections for businesses that write checks regularly?

Banks generally offer businesses a variety of check-protection services, including one known as “positive pay,” which compares the checks businesses issue with those that are presented to be cashed. If there’s a mismatch because the check has been altered, the problem can be caught before the check is cashed.

Similar protection services are offered for ACH or transactions that are debited directly from a business bank account.

What do I need to know about person-to-person payment platforms like Zelle and Venmo?

These apps — Zelle, Venmo, Cash App — are growing rapidly because they’re fast, easy to use and usually free. But they come with risks of their own, as my colleagues have reported. Treat them as if you were dealing with cash, transact only with those you trust and slow down when you’re using them. If the app asks you to verify the identity of the recipient, take the time to do so. Once you send money, you may not be able to get it back.

Zelle, through which consumers made 2.7 billion payments during the 12 months ending on Sept. 30, totaling \$758 billion, is the largest digital payment operator. It’s owned by seven of the nation’s largest financial institutions and is embedded inside the bank accounts that have access to it (about 2,100 financial institutions participate in the Zelle network, which means 165 million people with accounts can use it).

Federal regulators require servicers to refund customers money if an “unauthorized” transfer is made through these services, but not when an individual is scammed into authorizing a transaction. Last year, Zelle said it would require its participating banks to refund customers in some of those situations — namely, certain impostor scams. In these, a criminal may pose as an institution you already do business with, such as a bank, utility or mobile phone provider.

Ben Chance, chief fraud risk management officer at Early Warning Services, the company that operates the Zelle network, said those authorized transfers now posed the greatest threat.

“Think of it like cash,” Mr. Chance said. “If someone is pressuring you to make a decision rapidly, this the time to step back.”